AFRL-IF-RS-TR-2003-71
Final Technical Report
April 2003

MULTI-DIMENSIONAL SECURITY MANAGEMENT AND ENFORCEMENT SYSTEM (MSMES)

BBN Technologies

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. J525

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the U.S. Government.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2003-71 has been reviewed and is approved for publication.

APPROVED:

SCOTT S. SHYNE
Project Engineer

FOR THE DIRECTOR:

WARREN H. DEBANY, Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
APRIL 2003

3. REPORT TYPE AND DATES COVERED
Final Apr 00 – Oct 02

4. TITLE AND SUBTITLE
MULTI-DIMENSIONAL SECURITY MANAGEMENT AND ENFORCEMENT SYSTEM (MSMES)

5. FUNDING NUMBERS
C - F30602-00-C-0062
PE - 62301E
PR - J525
TA - 33
WU - A1

6. AUTHOR(S)
Matthew Condell, Charles Lynn, Alex Colvin, and David Waitzman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
BBN Technologies
10 Moulton Street
Cambridge Massachusetts 02138

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington Virginia 22203-1714

AFRL/IFGA
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2003-71

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Scott S. Shyne/IFGA/(315) 330-4819/ Scott.Shyne@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

Multi-dimensional Security Management and Enforcement (MSME). The project is a 27-month effort to develop a system that will allow coalition partners to determine if their existing security policies can support the communication requirements of the coalition before the communications are required by focusing on policy abstraction, policy exchange, policy resolution, and policy monitoring. This report includes MSME accomplishments, results, lessons learned, and documented output.

14. SUBJECT TERMS
Security Policy Management, Dynamic Coalitions, Policy Resolution, Policy Negotiation, IP security

15. NUMBER OF PAGES
70

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Contents

1 Summary **1**
1.1 Objectives 1
1.2 Results 1
1.3 Roadmap 2

2 MSME Documentation **2**
2.1 Requirements 2
2.2 Architecture 2
2.3 Design 2
2.4 Software Documentation 3
2.5 Published Papers 3

3 MSME Prototype **3**
3.1 Components 3
3.1.1 Policy Language 3
3.1.2 Policy Management Tool 4
3.1.3 Compilation 5
3.1.4 Exchange Protocol 6
3.1.5 Resolution 6
3.1.6 Monitoring/Reconciliation 8
3.1.7 Links to PBSM 9
3.2 Testing 9

4 Collaborations and Technology Transfer **10**
4.1 Telcordia/DC-PREMISYS 10
4.2 ISI/DEFCN 10
4.3 Austrailian DSTO 11
4.4 IETF 11
4.5 Future Possibilities 11

5 Lessons Learned **11**
5.1 Nested Policy Sets 11
5.2 Abstraction 12
5.3 Security Policy Complexity 12
5.4 Real User Experience 12

A Manual Pages **14**
A.1 plabind 14
A.2 plamodel 14
A.3 placheck 15
A.4 placover 16
A.5 plaresolve 16
A.6 plaresolvec 17
A.7 plaresolved 18
A.8 libplaresolve 18
A.9 sendmsme 20
A.10 plal2spsl 20
A.11 MSME CGI Conifguration 21

B Compilation **22**
B.1 Inconsistent PLA 22
B.2 Error Output 23
B.3 Consistent PLA 23

C Resolution **24**
C.1 Coalition Policies 25
C.2 Partner A: Abstract Rules 25
C.3 Partner A: Binding Library 26
C.4 Partner A: PLA 27
C.5 Partner C: PLA 28
C.6 Partner G: PLA 30
C.7 RPLA 31

D Monitoring **46**
D.1 PLA 1 46
D.2 PLA 2 48
D.3 RPLA 50
D.4 Reconcile with Correct RPLA 52
D.5 Incorrect RPLA 1 53
D.6 Reconcile with Incorrect RPLA 1 55
D.7 Incorrect RPLA 2 55
D.8 Reconcile with Incorrect RPLA 2 56

E PLAL to SPSL Conversion **57**
E.1 RPLA in PLAL 57
E.2 RPLA Converted to SPSL 62

List of Figures

1 Plague opening screen 4
2 PLA coalition header editor 4
3 PLA global dictionary editor 5
4 PLA policy editor 5
5 PLA source viewing window 6

1 Summary

The Multidimensional Security Management and Enforcement (MSME) system developed by BBN is a security policy management system that facilitates the resolution of policy requirements among the partners in a coalition.

This report describes the work performed as part of the project, results and output of the project, and lessons learned.

1.1 Objectives

As part of the MSME project, BBN architected, designed, and prototyped the services necessary for coalition members to define and resolve the security policies for communications required to complete the coalition's mission objectives. The resolution process and the enforcement of the policies is monitored for consistency and correctness.

BBN's MSME system created a means of negotiating security policies for dynamic coalitions through policy abstraction, exchange, resolution, and monitoring. Policies are defined at a high-level where mission planners can specify it as abstract, mission-related policy requirements. These high-level policies are then bound to one or more concrete policy contexts (e.g. IPsec, TLS). Policies are exchanged among coalition partners where they are resolved to determine the commonly supported mechanisms for the high-level requirements. The process is monitored to insure that the policies are resolved consistently and that partners enforce the resolved policies correctly.

BBN realized this process through the following components of the MSME architecture:

(R)PLA The Policy Level Agreement (PLA) [9, 5] provides the means for a partner to express its high-level security requirements through abstract assets and services. It also provides the means to define bindings that map the abstract names to concrete values. The Resolved PLA (RPLA) is similar to a PLA, but is the result of the resolution process.

Compilation Compilation [12, 1] creates a PLA from a set of abstract policies by collecting relevant bindings from local databases and checking the self-consistency of the PLA.

PLA Exchange Protocol Protocol [7] for exchanging PLAs among partners.

Resolution Resolution [2] merges PLAs from partners to generate and RPLA containing the commonly supported policies and mechanisms.

Reconciliation Reconciliation [17] validates that an RPLA does not violate local policies and identifies any places where the RPLA differs from local policies.

Policy Management Tool The PMT is the user interface to help write policies and initiate other processes.

Monitoring Monitoring [17] confirms consistent RPLAs are in use across the coalition, policy enforcement/decision points are correctly configured and communications are correctly protected. Monitoring is limited by mutual distrust between partners and encrypted messages.

When problems are detected, they must be reported, but manual intervention is required to fix most problems.

1.2 Results

BBN delivered requirements, architecture and design documents (Section 2) that described MSME's solution to the problem of security policy negotiation for dynamic coalitions. BBN also produced a prototype (Section 3) of the proposed MSME system that supports IPsec and TLS security contexts. BBN has promoted MSME as a solution for other projects that require inter-partner policy negotiation.

The prototype and project documentation has been made publicly available on the project website: http://www.ir.bbn.com/projects/msme/.

1.3 Roadmap

The remainder of this report discusses the results of the MSME project.

Section 2 provides an overview of the documents produced as part of the MSME project. These documents describe MSME's requirements, architecture, and design. Together, they provide a more in-depth description than is the focus of this report.

Section 3 describes the prototype of the MSME system that BBN produced. It describes each of the components that were implemented. It discusses issues with the implementation and changes to the design that resulted from those issues.

Section 4 describes some of the collaboration work BBN did with other projects in the Dynamic Coalitions program and what insights those discussions provided to our understanding of MSME.

Section 5 describes some of the lessons learned from MSME that should be considered by future researchers in the policy management field.

The appendices provide supporting documentation for the sections described above. Appendix A provides the manual pages describing each of the software components and how to use them. Appendix B provides examples of the compilation component input and output. Similarly, Appendices C, D, and E provide inputs and outputs for the resolution, monitoring, and PLAL to SPSL converter components, respectively.

2 MSME Documentation

This section describes the documents produced by BBN as part of the MSME project. This section is based on the *MSME Document Roadmap* [3] document which describes the relationships between the MSME document suite.

2.1 Requirements

Requirements for the Multidimensional Security Management and Enforcement (MSME) System [16] describes the requirements for the MSME system that have been used to guide the architecture and design.

2.2 Architecture

The overall MSME architecture is defined in the document, *MSME Architecture* [6]. This document provides the full picture of the MSME system.

However, several of the components of the architecture are discussed in documents focused on a single component or issue. These documents provide insights into the overall architecture and design.

Resolution *Policy Resolution Architectures* [10] discusses requirements and design considerations for policy resolution. It also discusses the tradeoffs between centralized and distributed resolution.

Protocol *Protocol Considerations for MSME* [13] discusses several issues related to designing a protocol to transport MSME messages and the pros and cons of several existing protocols.

Security abstraction layer *Security Abstraction Layer Architecture for MSME Integration (SALAMI)* [9] describes an architecture for specifying high-level policy agreements and mapping them to device-level mechanisms. This is the foundation for the PLA language design. *Schemata for Security Abstraction Layer Databases* [8] describes the policy information which databases must be able to provide in order to support the security abstraction layer.

2.3 Design

Each component of the MSME architecture is described in its own design document. These documents describe implementations, algorithms, and other information about the design of the components.

TLS model *A data model and language representation for SSL/TLS policies* [11] describes the policy model for SSL/TLS policies in a format similar to SPSL which describes IPsec policies. This model was written to use as a basis for the TLS description in the PLA language.

PLA Language *Policy Level Agreement Language (PLAL)* [5] describes and XML-based language for expressing policy level agreements (PLA). It is based on the security abstraction layer.

Compilation *COMPILER-NOTES* [1] describes the implementation of the MSME compiler. *MSME Policy Compilation* [12] is a deprecated document which describes the compilation process and the algorithms which implement compilation. The latter document is included since it provides a high-level view of the compilation process, although the algorithms are not being used.

Monitoring *MSME: Monitoring Design* [17] describes monitoring in the MSME system and surveys possible techniques currently available and those that may be available in the future. It lays out a few aspects of monitoring to implement as part of MSME.

Protocol *Transfer Protocols for MSME* [7] defines the finite state machine for the MSME exchange protcol and outlines a couple of means to implement it.

Resolution *Coalition Policy Resolution Algorithm Design* [2] describes the algorithms for coalition resolution and a couple of optimizations to make resolution more efficient.

2.4 Software Documentation

Documentation for the software components of the system is provided in the form of man pages which are provided with the MSME system and are reproduced in Appendix A.

2.5 Published Papers

Multidimensional Security Policy Management for Dynamic Coalitions [14] that describes MSME's architecture was published in the proceedings of DISCEX II. *Multidimensional Security Policy Management and Enhancements for IP Security Policy* [4] was presented as an internet draft to the IP Security Policy (IPSP) working group of the IETF. The draft was presented at the IPSP working group meeting at IETF 52 in Salt Lake City.

3 MSME Prototype

BBN implemented prototypes of each of the components of the MSME architecture. This section discusses the prototypes developed and how the prototyping affected the design. Results of testing the prototype are also discussed.

The prototype was demonstrated at the PI meetings in January and July 2002.

Manual pages that describe how to use the components described here are included in Appendix A.

3.1 Components

3.1.1 Policy Language

Partners require a common (at least pairwise) language in order to communicate their security policies. MSME developed the Policy Level Agreement Language (PLAL) [5] to serve this purpose. Originally we proposed to extend the Security Policy Specification Language (SPSL) that we developed for the DARPA-sponsored PBSM [15] project. However, extending SPSL required modifying a custom parser and SPSL required extensive modification to support policy abstraction, TLS policies, and coalition support. PLAL was developed using XML since a variety of tools are publicly available to process XML, allowing relatively easy prototyping for the language. However, XML provides little syntax checking capabilities so the prototype currently lacks much of this support.

PLAL was designed to be a very expressive language to allow very detailed and complex policies to be defined. However, the expressiveness came at a significant complexity cost that will be discussed further in Section 5.

The MSME prototype contains a PLAL parser library which has interfaces for C and TCL. The parser uses the freely available XML processing tool, libxml for the parsing and assembles the parsed data in structures for use by other components.

3.1.2 Policy Management Tool

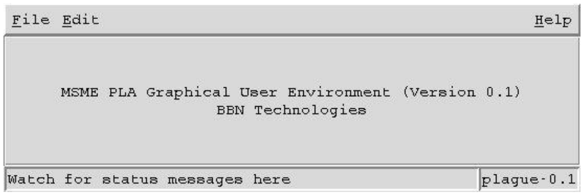
Plague (the Policy Level Agreement Graphical User Environment) is MSME's policy management tool. Plague provides a graphical environment for creating PLAs and an interface for performing compilation and initiating resolution by sending a PLA to a resolver to be resolved.

Plague is built with the open source TCL/TK and TIX packages. It takes advantage of XMLs tree structure and builds the editing tool from the PLAL DTD, so the editor changes as the DTD changes. Menu options initiate compilation and send the PLA to a resolver to perform resolution.

The interface that plague provides would need to be simplified for operational use, preferably with input from end users who need to be able to understand the interface. Discussions with some users at PI meetings suggest that a spreadsheet-like interface may be more appropriate than what is presented.

Additional features that would be good to integrate to make plague more user friendly would be better integration between the editor and compilation/resolution functions that would highlight problematic policy rules in the editor after the functions return to show the user where errors exist that must be corrected.

Figures 3.1.2, 3.1.2, 3.1.2, 3.1.2, and 3.1.2 show several snapshots of plague.

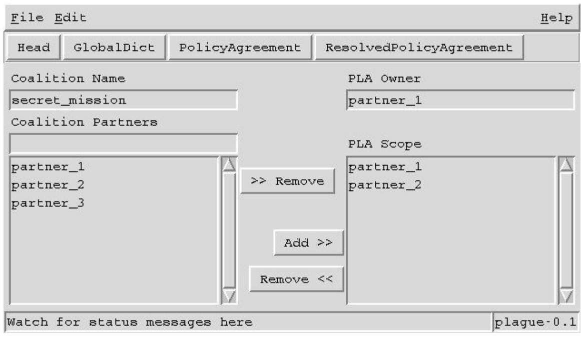


MSME PLA Graphical User Environment (Version 0.1)
BBN Technologies

Watch for status messages here

plague-0.1

Figure 1: Plague opening screen



Coalition Name: secret_mission

PLA Owner: partner_1

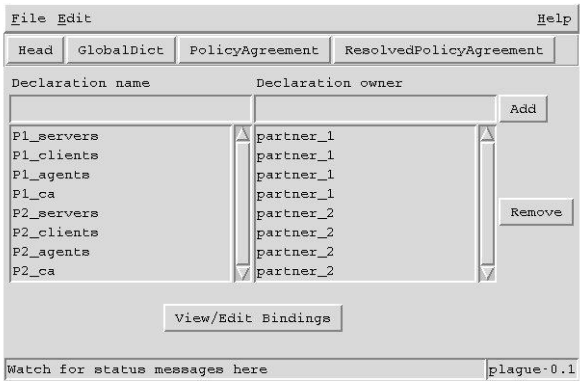
Coalition Partners:
partner_1
partner_2
partner_3

PLA Scope:
partner_1
partner_2

Watch for status messages here

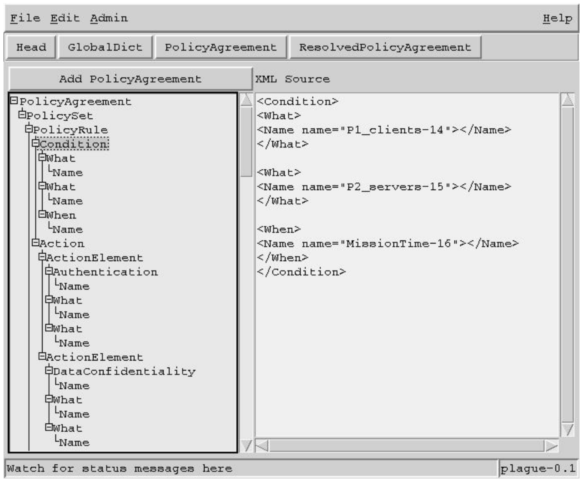
plague-0.1

Figure 2: PLA coalition header editor



Declaration name	Declaration owner
P1_servers	partner_1
P1_clients	partner_1
P1_agents	partner_1
P1_ca	partner_1
P2_servers	partner_2
P2_clients	partner_2
P2_agents	partner_2
P2_ca	partner_2

Figure 3: PLA global dictionary editor



```
PolicyAgreement
 PolicySet
  PolicyRule
   Condition
    What
     Name
    What
     Name
    When
     Name
   Action
    ActionElement
     Authentication
      Name
     What
      Name
     What
      Name
    ActionElement
     DataConfidentiality
      Name
     What
      Name
     What
      Name
```

```
<Condition>
<What>
<Name name="P1_clients-14"></Name>
</What>

<What>
<Name name="P2_servers-15"></Name>
</What>

<When>
<Name name="MissionTime-16"></Name>
</When>
</Condition>
```

Figure 4: PLA policy editor

3.1.3 Compilation

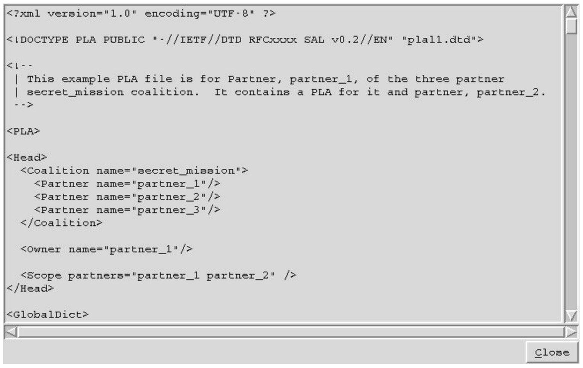
The MSME "compiler" takes PLAs and libraries of bindings and produces a PLA which includes all relevant bindings. The compiler can also check the consistency of PLA rules to determine whether any rules have conflicting actions.

As we started to implement the compiler, the original design for the compiler [12] was discovered to contain several bugs in the algorithms, though the general goal and concepts were sound. We decided to abandon most of those algorithms (though some were later used as part of resolution) in favor for implementing compilation as a more traditional compiler [1]. This resulted in a cleaner and easier to extend implementation.

The compiler consists of three separate programs that work together to provide the compilation.

`plabind`, reads a PLA and binding libraries and rewrites the bindings. It renames the names in <`Name`> and <`Binding`> elements so that bindings in different scopes have distinct names. The resulting PLA has only global <`Binding`> elements in the <`GlobalDict`> and <`PolicyAgreement`> elements, and is suitable for resolution. This pass looks like the front end of a traditional compiler.

`plamodel`, takes an input PLA produced by `plabind` or a resolved PLA, and translates it into a regular (and more verbose) notation that describes possible configurations. This pass looks like the back end (code



```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "pla11.dtd">

<!--
 | This example PLA file is for Partner, partner_1, of the three partner
 | secret_mission coalition.  It contains a PLA for it and partner, partner_2.
 -->

<PLA>

<Head>
  <Coalition name="secret_mission">
    <Partner name="partner_1"/>
    <Partner name="partner_2"/>
    <Partner name="partner_3"/>
  </Coalition>

  <Owner name="partner_1"/>

  <Scope partners="partner_1 partner_2" />
</Head>

<GlobalDict>
```

Figure 5: PLA source viewing window

generation) of a traditional compiler.

placheck, takes the translated expressions and computes all possible conditions and their corresponding actions, looking for conflicts among the actions. This part looks something like an interpreter.

The motivation is to isolate most of the model checking from details of the translation. Binding and translation deal with all the special cases of PLAL notation. The checker just needs to implement the right logical operations to combine the translated rules.

Compilation provides a solution to the NP complete canonical satisfiability problem, so for large policy sets it may not be practical to compile them. For complex rules there can be (exponentially) many possible configurations to consider. Because of this, evaluation proceeds depth-first so that only one configuration is considered at a time. The drawback to this strategy is that some configurations are considered repeatedly. In general, evaluation uses time to save space, since time limits are generally softer than space limits.

3.1.4 Exchange Protocol

MSME requires a protocol to exchange (R)PLAs between partners and resolvers. Originally we proposed to extend the Security Policy Protocol (SPP) from PBSM [15]. However, during design discussions we realized that we only needed a protocol to securely transfer policy files. Extending SPP to accomplish this would essentially implement a new protocol within SPP. With many file transfer protocols available, we decided that it would be more effective to use an existing protocol.

The protocol design we created included a finite state machine (FSM), that can be used with most any file transfer protocol, and how the (FSM) could be used in conjunction with HTTPS or secure e-mail.

BBN's prototype implemented the FSM as an HTTP CGI script in C. HTTP was used in the prototype since debugging and testing was easier than with HTTPS, however, the conversion between the two is trivial and mostly a configuration problem. The CGI script uses the freely available qDecoder and cURL packages to send and receive CGI form data. Several alternatives to qDecoder were tried, but were found to be incomplete or unreliable.

The prototype supports multiple coalition resolution architectures [10]. It can be configured (see Section A.11 for a sample configuration file) to operate in either a centralized or a distributed resolution architecture.

3.1.5 Resolution

The resolution module of the prototype has several programs associated with it that provide different interfaces to it, however they all use the same back-end code. plaresolve provides a command-line interface that allows a user to specify a set of PLAs to resolve on the command-line. plaresolved is a daemon that processes commands from a client and interfaces with the resolution algorithm implementation. libplaresolve is a library that contains a set of client routines to interface with plaresolved. The library is used for both the exchange protocol FSM implementation and `plaresolvec`. `plaresolvec` is a command-line client to `plaresolved`.

The back-end of the code has three main components. The first is the code that intersects bindings. This is based on the policy rule intersecting code from PBSM, since it serves a similar purpose.

The second is the table of bindings, which stores and provides access to bindings, both from the PLAs and intersected bindings. Access is provided to the bindings both by name and by the names of the two bindings that were intersected to form the binding. The binding table is one area where the performance of the resolver can be improved by using better database structures and lookup algorithms since much of the resolution process is accomplished by lookups in this table. Performance may also be improved by having a separate binding table for each node in the resolving tree, instead of a single table.

Finally, there is the code which intersects the policy sets. This implements the algorithms described in [2]. These algorithms were influenced by problems discovered while implementing their original versions.

There were two main areas that were affected by the implementation. The first is the copying of policy rules while intersecting policy sets. When two policy sets are intersected, it is necessary to include the unmerged policy rules, along with the merged rules, in the answer so that those rules are not lost when intersecting with another PLA later in the resolution process. The unmerged rules are filtered out before producing the RPLA. The initial design included this in a limited manner – the unmerged rules in a rule set were copied when at least one pair of rules did merge – however, it turned out to be incomplete. Testing exposed this flaw and indicated that *all* all policy sets needed to be included in the output, whether or not any rules merged in that set, so that the conjunctive/disjunctive set relationship between the policy rules was correctly preserved.

So, the output of resolving two flattened (e.g. distributed and unnested to form a disjunctive set of conjunctive policy rules) PLAs:

$$\begin{aligned} PLA_1 &= PS_{1,1} \vee PS_{1,2} \vee \cdots \vee PS_{1,n} \\ PLA_2 &= PS_{2,1} \vee PS_{2,2} \vee \cdots \vee PS_{2,m} \end{aligned}$$

Where :

PS represents a conjunctive policy set, and
$\vee$ indicates conjunction.

is the disjunction of the conjunction of each pair of policy sets:

$$\begin{aligned} PLA_1 \cap PLA_2 = \quad & (PS_{1,1} \oplus PS_{2,1}) \vee (PS_{1,1} \oplus PS_{2,2}) \vee \cdots \vee (PS_{1,1} \oplus PS_{2,m}) \\ & (PS_{1,2} \oplus PS_{2,1}) \vee (PS_{1,2} \oplus PS_{2,2}) \vee \cdots \vee (PS_{1,2} \oplus PS_{2,m}) \\ & \vdots \\ & (PS_{1,n} \oplus PS_{2,1}) \vee (PS_{1,n} \oplus PS_{2,2}) \vee \cdots \vee (PS_{1,n} \oplus PS_{2,m}) \end{aligned}$$

Where :

PS represents a conjunctive policy set, and
$\vee$ indicates conjunction, and
$\oplus$ indicates a conjunction that includes the policy rules from both sets,
plus any policy rules created by intersecting the rules from both sets.

The second area influenced by the implementation was which of the two "basic" algorithms proposed in the design document is better to use. The released implementation follows the second basic algorithm with the tree-based optimization. Initially, we implemented the first basic algorithm we proposed, however testing revealed that it did not scale at all. Even the 10 PLA example described in Appendix C was infeasible for a reasonable desktop computer.

The difference between the two algorithms is how they deal with intersecting bindings. The first basic algorithm intersects each binding in a PLA with all the bindings currently processed (intersected and non-intersected bindings). The second algorithm intersected only intersected bindings as they were needed by the policy rule intersecting algorithms.

While initially it seemed like both algorithms require approximately the same number of binding intersections, since nearly every asset binding must be intersected with nearly every other asset binding in either case, this is not actually the case. Intersecting bindings requires saving the result of the intersection in the binding table. When merging many PLAs, this creates many intermediate intersections that are not necessary at any point in merging the policy rules. Additionally, many mechanism bindings may not need to be intersected, since not all asset bindings are likely to intersect.

Using the second algorithm, therefore, greatly reduces the exponential growth of the binding table that causes the first algorithm to scale poorly.

3.1.6 Monitoring/Reconciliation

Monitoring for MSME can be done at many levels, and it is likely that no one monitoring technique will offer a complete solution. The monitoring design document [17] discusses many monitoring technologies and how they may be used to monitor MSME and how policy enforcement points are enforcing the resolved policies. Monitoring is limited by communications being encrypted.

Many of the techniques available for monitoring are existing monitoring functions, such as SNMP, sniffing, and SENCOMM that can be used to gather information which then needs to be processed and compared to the resolved policy to determine if the policies are being adhered to.

While these monitoring techniques are a very important part of a total monitoring solution, MSME decided to focus on allowing partners to monitor the correctness of the resolution process. Two different monitoring functions are needed depending on if the resolution is done in a centralized or distributed manner.

When resolution is centralized, each partner need not completely trust the resolver to behave correctly. While the partner cannot completely verify that the resolution is correct, it can determine that the resolved PLA does not violate the policy it presented in the PLA and identify rules that were not resolved with other partners. The administrator can then attempt to resolve any problems with their counterparts at the other partners. This process is called resolution. The partner does have to have some trust in the resolver to correctly present globally defined bindings for which the partner does not know before the RPLA is presented.

When resolution is distributed among the partners, it is important that the partners share their RPLAs to allow them to confirm that they are all using equivalent RPLAs. This confirms that they all should be using the same policies to communicate. This checking ends up being very similar to reconciliation, the main difference is that it is a symmetric comparision (the RPLAs need to each be checked against the other), instead of a unidirectional comparison (comparing the PLA to the RPLA).

The MSME team had several implementation discussions about whether these monitoring techniques would be best implemented by basing it on the compilation or resolution code. While it would not have been too difficult to extend either of them to accomplish the task, reconciliation is more directly related to compilation, since it is a consistency check, only between two (R)PLAs instead of internal to one.

Being able to implement a solution using either compilation or resolution brings up the question about how much of the two components could be combined to share code, however there was not the opportunity to explore this idea further.

The first step to reconciliation is to compile the RPLA to make sure it is consistent. This step can be optimized for the case where most of the policy rules have overlapping conditions or the case where there are few overlaps. The performance difference between running a case for which it is optimized over a case for which it is unoptimized is several orders of magnitude. We chose to implement the optimization for the case where there are few overlaps, since it seems the most common case for policy rules. It would be possible to implement both optimizations and either provide a switch that allows the user to choose the correct optimization or detect which should be used automatically.

The second step is to determine if the RPLA covers all the rules in the PLA and report any problems. The number of checks can be exponential in the number of RPLA rules as it considers them in all possible combinations. Moreover, each step in the recurrence involves testing a conjunction of conditions and possible conjunction of actions. Since PLA conditions and actions tend to have many parts, these tests can be computationally expensive. As a result, these RPLA coverage tests are likely to be impractical even for moderate-size RPLAs.

We have considered possible solutions to make the problem more tractable but did not have time to explore them further. These include: reducing the scope of the problem by checking just for policy violations and not all places where the RPLA deviates from the PLA, checking for PLA rules used unaltered in the RPLA, taking advantage of global bindings and assume the relationship between the names and concrete values, and using a better model checker that uses better algorithms and doesn't recompute as many values. These are discussed in a bit more detail in the compiler notes document [1].

3.1.7 Links to PBSM

MSME by itself is not a complete security policy management solution. Once it returns an RPLA and it is reconciled, the partner needs to be able to use those policies to provision its policy enforcement points and use the policies for communications.

Our collaboration efforts were mostly focused on integrating with another system that would provision the policies. However, we had proposed to integrate MSME with the PBSM system [15] to negotiate the policies host-to-host and provision them as needed. PBSM was originally developed under FreeBSD 2.2.8, so it had to be ported to FreeBSD 4.3 to be compatible with MSME. It was believed that this was mostly a matter of porting some kernel modifications and since the majority of the code operated in user-space the porting would be straightforward. Between the two FreeBSD releases the KAME IPsec/IPv6 code that PBSM used had been integrated into FreeBSD. The necessary kernel modifications were made, however the user-space code was not easy to port due to modified IPsec/IPv6 structures supported by the kernel and other bit rot in the kernel and tools which PBSM relied upon. To complete the effort would have been too costly and take more time than could have been afforded.

Integrating MSME with any provisioning system would require the reconciled RPLA to be translated into a language understood by that system and loaded into that system. Despite not having a fully operational PBSM system, we were able to translate PLAL into PBSM's SPSL language and demonstrate that it would successfully load into PBSM's security server (which if fully working would then negotiate the loaded policy).

`plal2spsl` is the translator between the two languages. Because of differences between the languages, the translation is not complete. The most obvious difference is that SPSL only supports IPsec. Any non-IPsec contexts are ignored in the translation. SPSL also interprets rules differently, since it has no means to specify the conjunctive/relationships between policies and decorrelates the policy rules. This may lead to different interpretations of the policy rules than was intended by the PLAL. Signatures are required on each policy rule in SPSL which are not provided in our implementation, but could be added using a private key certificate that belongs to the translator of the rules.

3.2 Testing

Each component was tested separately and together as a system, however, since the communication between the components was mostly in the form of a (R)PLA file, component tests generally insured a correct systems test. Examples of compilation, resolution, reconciliation, and PLAL to SPSL translation are included in the appendices.

Many modifications to the design and implementation that resulted from the testing and areas that we've identified that can be improved are discussed above.

Testing was mostly conducted using two main examples, a three PLA example (shown in Appendix E) and a ten PLA example (described in Appendix C). Smaller examples were created to test particular features of components, such as those shown in appendices B and D. A larger set of example PLAs was not created due to time constraints and the difficulty in creating complex policies (see Section 5.

4 Collaborations and Technology Transfer

Since MSME produced a prototype that dealt with inter-partner policy resolution, but did not produce a back end to provision policies to end systems, there was an obvious focus of where we could collaborate with other projects.

BBN talked with several other projects about collaboration and some of the issues and results are discussed here.

4.1 Telcordia/DC-PREMISYS

Through consultation with the program manager, we decided to focus our collaboration efforts on the DC-PREMYSIS project.

We installed and set up the version of DC-PREMISYS that was handed out at the January 2002 PI meeting. We used it to familiarize ourself with their system and to determine how a collaboration would be most effective. Our impression is that DC-PREMISYS's IPsec policies could be turned into MSME policies, resolved, translated back to DC-PREMISYS where they then can be provisioned. Since MSME is focused on security policy, it could only resolve the IPsec filter rules in the policy and not the rest of the router configuration information contained in the DC-PREMISYS policies.

The obvious means of interfacing with DC-PREMISYS would be through PLAL. Our initial thought was to translate policies from DC-PREMISYS's Java IPsec router configuration programs to PLAL and back. To this end we have a prototype of a translator from DC-PREMISYS's Java IPsec policies (an example was included in their release) to PLAL. The translator was not full featured due to lack of documentation from Telcordia on the full set of IPsec policies that they could express.

Further experience with the system, however led us to believe that a better way of interfacing with DC-PREMISYS would be to extract policy from its LDAP database and dump the resolved policies back into the database. Some work was accomplished towards that end, however funding constraints required that we abandon that effort in a very early stage.

4.2 ISI/DEFCN

BBN talked a bit with ISI about integrating MSME with their DEFCN project. While the collaboration was not possible because of resource limits, it did give us an opportunity to do the thought exercise about how to extend MSME.

DEFCN's policies contained security contexts not supported by MSME's prototype, including Kerberos and access control. If we were to collaborate, it would be necessary to extend the prototype to support these contexts.

We determined that the following changes would have to occur to support the new contexts:

- Extend PLAL to support the new contexts. PLAL's XML nature would have made this fairly easy once the new contexts had been modeled so we understood what needed to be added. An access control service already exists, so it would be easy to integrate the new contexts in it.

- Extend resolution to intersect contexts. The resolver would have to be extended to be able to support intersecting bindings in the Kerberos and access control contexts. The rest of the resolution process should not be affected.

- Extend compilation to model and check contexts. This mostly involves extending the compilation tables to understand how to process the new contexts.

4.3 Austrailian DSTO

Mathew Elliot of the Australian Defense Science and Technology Organization (DSTO) has worked on testing our first release. He contacted us in late March 2002 with some questions to which we promptly replied. We have provided assistance and have offered our help, as needed.

4.4 IETF

In December 2001, BBN submitted and presented an Internet Draft to the IETF's IPSP working group that described MSME's architecture and how some of MSME's work could be used to enhance the work of the working group. Unfortunately, the working group is proceeding very slowly and it is unclear whether or not any of the work presented will be adopted.

4.5 Future Possibilities

BBN has been working to make MSME known to other programs that may be interested in it. These include:

- NICCI - As part of a proposal to this upcoming program.
- MilSatCom - BBN introduced MSME as an emerging technology that would be useful for MilSatCom through their recent Transformational Study with Industry (TSI).
- JV 2020 - BBN believes MSME provides a model for Joint Vision 2020's network-centric view that stresses interaction with foreign partners, NGOs, and civilian agencies and is exploring options in that area.

5 Lessons Learned

The most important lesson learned from MSME relates to security policy complexity, both MSME specific issues and general issues.

MSME is built on BBN's experience of designing SPSL when designing PLAL, using a similar design for concrete policy expressions, but adding a TLS context and abstracting the policies so that a high level rule can map to multiple security contexts. Additionally, PLAL changed how policy rules relate to each other by allowing them to be grouped into conjunctive and disjunctive sets of rules. Some of these changes were made to accomplish MSME's goals, while some were added to make a more expressive language.

5.1 Nested Policy Sets

Some of these changes hurt the utility of PLAL and some have the potential to help make it easier to use.

In retrospect, one part of PLAL that we would change is allowing nested policy sets. It is the feature of the lanuage that adds the most unneeded complexity. While it does allow the definition of complex relationships between policy rules, it adds a lot of processing complexity and makes the policies difficult to understand.

The processing complexity comes from multiple places. The nested policy sets lead to a larger number of policy rules to be processed. These rules are introduced at two places in the resolution process. The first is when the policy of an incoming PLA is flattened [12]. The flattening involves distributing and unnesting rule sets which involve the copying of rules. The second occurs when PLAs are intersected and each set of one PLA must be merged with every set of the other PLA (described in Section 3.1.5). This potential for an explosion of duplicate policy rules leads to many more rule intersections than might otherwise be required.

Nesting policy rules adds complexity by prohibiting the use of decorrelation to try to develop a more efficient resolving process, since it is not clear how to decorrelate nested policy rules. Further complexity has been alluded to previously in translating PLAL to other policy languages, since, like SPSL, few other languages support nesting. It is not possible to preserve the meaning of the nested rules when translating them into languages supported by provisioning systems, so some of the benefit of the nesting is lost in the end. (Not all the benefit is lost, since providing options is useful for resolving policies, but if the resolution results in there being multiple options to support a service, that information may be lost in the translation.)

Nesting also makes policies difficult to understand. While one layer of nesting may be useful (do X and either do Y or Z), more layers become increasingly difficult for an administrator to interpret the policy that is being represented. As it becomes more difficult for the administrator to understand the policy, it becomes increasingly likely that the policy does not say what is intended.

5.2 Abstraction

The level of policy abstraction provided by MSME has the potential to be either helpful or a hinderance to policy writers, depending on how it is used.

If there is a lot of reuse of asset and mechanism bindings, either within a PLA or even between PLAs for different coalitions, it could make policy rules easier to write. If the same bindings can be used for different coalitions, binding databases can be developed to facilitate policy writing. However, if bindings are basically used only once, they may end up being more of a hinderance, since it is more layers to write for each policy rule. It is possible for the user interface to hide this added complexity, if it is designed for the particular administrator who will be writing this type of policy.

5.3 Security Policy Complexity

PLAL also suffers from a general complexity that is inherent in security policies. These policies have many knobs to turn (security context, services, algorithms, key lengths, expirations, etc.) which allows an administrator to fine tune the required protection on every potential communication.

Since security policies are inherently complex, the user interface must be able to make writing a policy tractable to the administrator. It may do this through user-settable defaults, policy abstraction similar to what is in PLAL, and other methods.

MSME's PMT falls short on this, since it was not the focus of the project, however our experience with it makes it clear that a lot of work needs to be put into a user interface to make it reasonably easy for administrators to write policies. Without a powerful user interface it is too easy to create a policy other than what was intended which may either leave a system vulnerable or make necessary communications impossible.

5.4 Real User Experience

A final lesson is about the need to infuse projects like MSME with some idea about how a user might really use the system to improve the value of the prototypes. There are several places where we saw such input would be useful.

Designing a user interface is the most obvious place where such input is crucial. The interface needs to be useable and facilitate the type of policies that are going to be most often handled.

However, there are a variety of other places where the system design would benefit from knowing the nature of the policies that would likely be used in the system. For example, are nested policies a useful concept in practice? Are policies likely to reuse mechanism bindings and/or asset bindings often within a PLA? Does a partner's policy generally contain tens, hundreds, or thousands of policy rules? Knowing answers to these kinds of issues, can help make architecture, design, and implementation tradeoff decisions more useful to the eventual users.

References

[1] A. Colvin. MSME Compiler Notes. March 2002.

[2] M. Condell. Coalition Policy Resolution Algorithm Design. December 2001.

[3] M. Condell. MSME Document Roadmap. December 2001.

[4] M. Condell. Multidimensional Security Policy Management and Enhancements for IP Security Policy. Internet Draft draft-ietf-ipsp-00.txt, Internet Engineering Task Force, November 2001.

[5] M. Condell and R. Krishnan. Policy Level Agreement Language. December 2001.

[6] M. Condell, G. Patz, R. Krishnan, and C. Lynn. MSME Architecture. December 2001.

[7] R. Kishnan. Transfer Protocols for MSME. December 2001.

[8] R. Krishnan. Schemata for Security Abstaction Layer Databases. March 2001.

[9] R. Krishnan. Security Abstaction Layer Architecture for MSME Integration (SALAMI). November 2001.

[10] C. Lynn. Policy Resolution Architectures. October 2000.

[11] G. Patz. A data model and language representation for SSL/TLS policies. November 2000.

[12] G. Patz. MSME Policy Compilation. April 2001, Depreciated.

[13] G. Patz. Protocol considerations for MSME. October 2000.

[14] Geva Patz, Matthew Condell, Rajesh Krishnan, and Luis Sanchez. Multidimensional Security Policy Management for Dynamic Coalitions. In *Proceedings of DARPA Information Survivability Conference and EXposition 2001 (DISCEX II)*, June 2001.

[15] L. Sanchez and M. Condell et al. Policy based dynamic security management: Final technical report. DARPA Contract No. F19628-97-C-0060, August 1999.

[16] L. Sanchez, D. Waitzman, M. Condell, R. Krishnan, and C. Lynn. Requirements for the Multidimensional Security Management and Enforcement (MSME) System. November 2000.

[17] D. Waitzman, M. Condell, and L. Sanchez. MSME: Monitoring Design. May 2001.

A Manual Pages

A.1 plabind

Name

plabind - PLA library binding

Synopsis

plabind [**-names**] [**-debug**] [**-format** *format-string*] [**-rpla** *resolved-policy*] *library ...*

Description

plabind reads a PLA from *stdin*, locates bindings in libraries and RPLAs and inserts them into the PLA. It renames local bindings to unique names and discards unreferenced local bindings. The result, a PLA with external references resolved, is printed on *stdout*.

-names] Prints a list of included bindings on *stderr*.

-debug] Be verbose with debugging information.

-format *format-string*] changes the format used for renaming from the default "%s-%d".

-rpla *resolved-policy*] takes global bindings from the **ResolvedPolicyAgreement** element of a resolved policy. These bindings apply after library bindings.

Library

files are XML files with a single root element containing a list of **Binding** elements.

Static scoping rules apply, with bindings from inner elements taking precedence over bindings from outer elements. Library bindings are applied after any bindings in the PLA. PLA and library bindings take precedence over **GlobalDict** or **ResolvedPolicyAgreement** bindings. Local bindings are visible only in their parent element, but may be referenced by any sibling element.

plabind warns of references to undefined and undeclared names. The exit status is negative if there are any such references.

See Also

plamodel(8) placheck(8) placover(8)

Bugs

A name should not be bound in more than one library.

Authors

Alex Colvin for BBNT

A.2 plamodel

Name

plamodel - PLA model translation

Synopsis

plamodel [**-rpla**] [**-dual**] [**-warn**] [**-quiet**] [**-simple**]

Description

plamodel reads a bound PLA (as produced by plabind(8)) from *stdin* and produces an abstract description of the PLA rules on *stdout*. This description is suitable for consistency checking by placheck(8) or placover(8).

-rpla] translates the **ResolvedPolicyAgreement** element of a resolved PLA instead of the **PolicyAgreement**.

-dual] includes the logical complements of rule conditions and actions, as required for resolution checking.

-simple] applies some algebraic simplifications to the output to make it more concise.

-warn] warns of undefined global names and other constructs that may be difficult to model.

-quiet] turns off most warnings.

See Also

plabind(8) placheck(8) placover(8)

Bugs

plamodel does not implement the IKE and X509 parts of PLAL, and may not agree with other interpretations of some PLAL features.

Authors

Alex Colvin for BBNT

A.3 placheck

Name

placheck - PLA consistency checking

Synopsis

placheck [**-quiet**] [**-heap**] [**-sets**] [**-acts**] [**-conds**] [**-confs**]

Description

placheck reads an abstract model of a PLA produced by plamodel(8) from *stdin* and identifies conflicting rules. Rules conflict if they appear in a conjunctive rule set, have conditions that intersect, and have actions that do not intersect.

-quiet] supresses printing statistics at the end of checking.

-heap] traces memory manager activity.

-sets] traces rulesets produced by distributing rule conjunctions over disjunctions.

-conds] traces possible conditions for rules.

-acts] traces possible actions by rules.

-confs] traces the evaluation of possible configurations.

Tracing displays the XPath of these components and their top-level operator, but does not display their contents.

placheck uses a depth-first algorithm to explore the state space, making efficient use of memory at the cost of increased runtime. Summary statistics printed at the end of checking indicate the size of the state space explored. In pathalogical cases this is exponential in the number of rules.

placheck exits with zero status if there are no rule conflicts.

See Also

plabind(8) plamodel(8) placover(8)

Bugs

placheck may generate many subsets of conjunctive rules for consideration. In the degenerate case, it considers all subset.

placheck may not correctly handle disjunctive sets of rules where some rule sets are inconsistent.

Authors

Alex Colvin for BBNT

A.4 placover

Name

placover - PLA/RPLA coverage checking

Synopsis

placover [**-quiet**] [**-heap**] [**-sets**] [**-acts**] [**-conds**] [**-confs**] [**-live**] [**-safe**]

Description

placover reads an abstract description of a PLA and RPLA produced by plamodel(8) from *stdin* and tests the RPLA's coverage of PLA rules.

A PLA rule's condition must be satisfied by at least one RPLA rule's condition. The action of all applicable RPLA rules must be at least as restrictive as the actions of the PLA rule.

-quiet] supresses printing statistics at the end of checking.

-heap] traces memory manager activity.

-sets] traces rulesets produced by distributing rule conjunctions over disjunctions.

-conds] traces possible conditions for rules.

-acts] traces possible actions by rules.

-confs] traces the evaluation of possible configurations.

-live] lists the RPLA rules in a set that implement each PLA rule.

-safe] shows the unsafe action and its condition.

Tracing displays the XPath of these components and their top-level operator, but does not display their contents.

The input to **placover** is an XML tree rooted in a **COVER** element containing the PLA followed by the RPLA. Both the PLA and RPLA must be translated with the **placover** *-dual* option.

placover uses a depth-first algorithm to explore the state space, making efficient use of memory at the cost of increased runtime. Summary statistics printed at the end of checking indicate the size of the state space explored. In pathalogical cases this is exponential in the number of rules.

placover exits with zero status if there are no rule conflicts.

See Also

plabind(8) plamodel(8) placheck(8)

Bugs

placover needs to consider many combinations of terms from the PLA with terms and their logical complements from the RPLA. The number of such combinations increases rapidly with the number of rules in the RPLA.

placover may not correctly handle disjunctive sets of rules where some rule sets are inconsistent.

Authors

Alex Colvin for BBNT

A.5 plaresolve

Name

plaresolve - Command-line PLA resolver

Synopsis

plaresolve [**-v**] [**-s**] [**-o** *output-filename*] [**-d** *dtd-filename*] *partner pla-filename ...*

Description

plaresolve Resolves a list of policy level agreements (PLAs) by finding their commonly supported policies. **plaresolve** takes the name of the *partner* which is doing the resolving and a list of *pla-filenames*, the files containing the PLAs to be resolved. The resolved PLA will be written to standard out.

-v] Be verbose with debugging information.

-s] Produce output that is compatible with plal2spsl(8). Output is similar, but a bit less optimized since it requires that bindings to different contexts have different names.

-o *output-filename*] Specifies a filename to write the resolved PLA output instead of *stdout.*

-d *dtd-filename*] Uses the DTD specified by *dtd-filename* to validate the PLAs.

See Also

plaresolved(8) plaresolvec(8) libplaresolve(3)

Bugs

The current implementation doesn't handle scoped bindings correctly. Additionaly it doesn't handle the cases where two partners have named non-global bindings the same. However, the compilation functions distributed with MSME will ensure that these will not occur.

This implementaion does not merge concrete rules that are not a result of bindings.

This implementation doesn't merge AccessControl parameters.

Composite bindings may not work in some cases. This may partially be avoided by placing composite bindings that refer to other composite bindings later in the file than those that they reference.

There are several places where efficiency can be improved. Most notably, improving binding table lookups most likely would improve performance greatly.

Authors

Matthew Condell for BBNT

A.6 plaresolvec

Name

plaresolvec - PLA resolving client

Synopsis

plaresolvec [**-v**] [**-o** *output-filename*] *command data*

Description

plaresolvec is a client for the plaresolved(8) resolving daemon. The resolver sends incoming add, modify, or delete requests to the daemon with the appropriate data. It listens for a reply from the daemon and prints it to *stdout.* libplaresolve(3) describes the protocol used to communicate between the client and daemon.

-v] Be verbose with debugging information.

-o *output-filename*] Specifies a filename to write the resolved PLA output instead of *stdout.*

command may be one of the following:

add] *Add* indicates a new PLA to be added to the resolution. *data* is the filename containing the PLA to be added.

modify] *Modify* indicates a PLA to replace a current PLA in the resolution. *data* is the filename containing the PLA to replace the current one.

delete] *Delete* indicates a partner to remove from the resolution. *data* is the name of the partner that is to be removed.

get] *Get* requests the current RPLA. *data* is not used.

See Also

plaresolved(8) plaresolve(8) libplaresolve(3)

Authors

Matthew Condell for BBNT

A.7 plaresolved

Name

plaresolved - PLA resolving daemon

Synopsis

plaresolved [**-v**] [**-s**] [**-D**] [**-d** *dtd-filename*] [**-u** *user*] *partner*

Description

plaresolved is a daemon which resolves policy level agreements (PLAs) by finding their commonly supported policies. The resolver listens for incoming add, modify, or delete requests from a client on the UNIX domain port */tmp/msmeserv* When it receives a request, it resolves the PLA with the other PLAs currently active and returns the RPLA or an error. libplaresolve(3) describes the protocol used to communicate between the client and daemon.

-v] Be verbose with debugging information.

-s] Produce output that is compatible with plal2spsl(8). Output is similar, but a bit less optimized since it requires that bindings to different contexts have different names.

-D] Do not fork off the daemon.

-d *dtd-filename*] Use the DTD specified by *dtd-filename* to validate the PLAs.

-u *user*] The *user* to run the daemon. This should be set to the same user as the client that will access the daemon (e.g. HTTP server).

plaresolve also takes the name of the *partner* which is doing the resolving.

See Also

plaresolve(8) plaresolvec(8) libplaresolve(3)

Bugs

The current implementation doesn't handle scoped bindings correctly. Additionaly it doesn't handle the cases where two partners have named non-global bindings the same. However, the compilation functions distributed with MSME will ensure that these will not occur.

This implementaion does not merge concrete rules that are not a result of bindings.

This implementation doesn't merge AccessControl parameters.

Composite bindings may not work in some cases. This may partially be avoided by placing composite bindings that refer to other composite bindings later in the file than those that they reference.

There are several places where efficiency can be improved. Most notably, improving binding table lookups most likely would improve performance greatly.

Authors

Matthew Condell for BBNT

A.8 libplaresolve

Name

plares_init plares_finish libpla_send_msg libpla_recv_msg - PLA resolving library

Synopsis

#include<libplaresolve.h>

plares_handle plares_init();

void plares_finish(*plares_handle handle*);

int libpla_send_msg(*plares_handle handle*, *int opcode*, *int datalen*, *char *data*);

int libpla_recv_msg(*plares_handle handle*, *int *opcode*, *int *datalen*, *char **data*);

Description

The policy level agreement (PLA) resolving library contains functions for a client to connect to the resolving daemon, plaresolved(8).

Protocol

The client and the daemon communicate with the following protocol:

```
1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Op Code                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Data Length                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                            Data                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Opcode:

0] Error

1] Add PLA

2] Modify PLA

3] Delete PLA

4] Return RPLA

5] Get current RPLA

For opcode 0 data is error message For opCodes 1,2,4 data is a temporary filename where the (R)PLA is stored For opCode 3 data is the Partner name For opCode 5 data is not used

Functions

plares_init() initializes the client and prepares it to communicate with the daemon. It returns a handle which is required for the other library functions, so this function must be called before any other library routines.

libpla_send_msg() is used to send a message from the client to the daemon.

int libpla_send_msg(*plares_handle handle*, *int opcode*, *int datalen*, *char *data*)

libpla_send_msg() takes the handle created by the initialization function, one of the sending *opcodes* described below, the *data* that corresponds to the *opcode*, and the length of the data. It returns 1 if the message was sent successfully and -1 if the send fails.

libpla_recv_msg() waits for a reply from the daemon and returns it when it arrives.

int libpla_recv_msg(*plares_handle handle*, *int *opcode*, *int *datalen*, *char **data*)

libpla_recv_msg() takes the handle reated by the initialization function and waits for a reply from the daemon. When the reply is received it is parsed and the *opcode*, *datalen*, and *data* arguments are filled in with the data from the reply message. It returns 1 if the message was received successfully and -1 if the receive fails.

plares_finish() is used to clean up state set up by the initialization function, so should be called after all the sending and receiving is complete. It takes the handle from the initialization function as an argument.

Argument details

The handle points to information about the connection with the server:

typedef struct _plares_handle {
int fd;
struct sockaddr_un server;
} plares_handle;

There are several op-codes that may be sent or received:

MSME_OPCODE_ERROR] A return code indicating an error resolving the PLA. The data may contain text describing the error.

MSME_OPCODE_ADD] A sending code that requests the PLA contained in the file named in the data be added to the coalition's RPLA.

MSME_OPCODE_MODIFY] A sending code that requests the PLA contained in the file named in the data be used to replace the currently PLA for that partner.

MSME_OPCODE_DELETE] A sending code that requests the PLA corresponding to the partner that is named in the data be removed from the coalition's RPLA.

MSME_OPCODE_RPLA] A return code indicating that the file named in the data contains the resolved PLA that resulted from the corresponding request.

MSME_OPCODE_GET_RPLA] A sending code that requests that the resolver return the current RPLA.

See Also

plaresolved(8) plaresolvec(8)

Authors

Matthew Condell for BBNT

A.9 sendmsme

Name

sendmsme - Command-line client for the MSME protocol CGI program

Synopsis

sendmsme [**-v**] [**-o** *output-filename*] *localserver remoteserver command* [command-args]

Description

sendmsme is a client for the *msme.cgi* MSME protocol CGI program. It sends a message containing the *command* and optional *command-args* to the server. It listens for a reply from the protocol and prints it to *stdout*.

-v] Be verbose with debugging information.

-o *output-filename*] Specifies a filename to write the returned data instead of *stdout*.

command may be one of the following:

start] *Start* sends a start message to the CGI program which includes a new PLA to resolve. *command-args* is the filename containing the PLA to be added.

Authors

Matthew Condell for BBNT

A.10 plal2spsl

Name

plal2spsl - PLAL to SPSL convertor

Synopsis

plal2spsl PLAL_file_name DTD_file_name [*-debug*|*-DEBUG*]

-debug] Turns on mild debugging

-DEBUG] Turns on maximal debugging

Description

plal2spsl converts a PLAL language file containing resolved policy agreements into a PBSM SPSL language file. The SPSL form is send to stdout. Errors are sent to stderr. The optional debugging messages are sent to stdout but are prefaced with a hash sign to make them SPSL comments.

Configuration

plal2spsl has no configuration options and thus no configuration file.

Limitations

Many! Many PLAL elements are not handled. They may be parsed properly, with some level of validation, but are not converted and output to SPSL. These unhandled elements include: all TLS, all X509, KeyManagement, DigitalSignature, AccessControl, DataIntegrity, NonRepudiation, Transit, Compression, Steganography, RoutingControl, TrafficPadding, KeyManagement.

Does not generate SPSL associations nor any other SPSL object other than a policy.

Does not check <Encipherment> type field in any user of PLA_SM_Encipherment. We are assuming for now that the algorithms are correct with regards to the reversible_symmetric, etc. values. The referenced binding specifies the algorithms to use, in an <IPsecCipher> element. Do I need to know that certain algorithms are reversible_symmetric vs reversible_asymmetric va irreversible, and put the "filtered" algorithms in the SPSL file? Since <IPsecCipher> support arbitrary decimal values from RFC2407, how do I know ahead of time which have the right properties?

The not= attribute is not always handled.

Opaque protocols are not handled.

The role attribute is ignored in Whats in Conditions.

Generation of SPSL signatures is not implemented – but SPSL doesn't check them anyway.

Bugs

See limitations.

Author

David Waitzman for BBNT

A.11 MSME CGI Conifguration

```
# pla_location
#
#  location of the current pla for this partner
#
pla_location /usr/local/etc/pla

# rpla_location
#
#  location to place rplas when they are delivered
#
rpla_location /usr/local/etc/rpla

# log_location
#
#  location to place logging information. Default /var/log/msmelog.
#
log_location /var/log/msmelog

# local_url
#
#  URL of the msme.cgi program that is running locally so that
#  replies can be sent to it.
```

```
#
local_url https://my.local.server/cgi-bin/msme.cgi

# is_resolver
#
#  Indicates whether or not this server does resolution.
#  1 indicates it does resolution, 0 indicates it does not.
#  Default is 1.
is_resolver 1

# distributed_resolution
#
#  Indicates whether or not the coalition does distributed resolution.
#  1 indicates it does distributed resolution, 0 indicates it does not.
#  Default is 1.
distributed_resolution 1

# resolver
#
#  URL of resolvers to send PLAs.
#  If centralized resolution is being done, this is just the coalition
#  resolver.  If decentralized resolution is being done, this will be
#  the URL of each partner's resovler.
#
resolver https://server.partner1.com/cgi-bin/msme.cgi
resolver https://server.partner2.com/cgi-bin/msme.cgi
resolver https://server.partner3.com/cgi-bin/msme.cgi
resolver https://server.partner4.com/cgi-bin/msme.cgi
```

B Compilation

This appendix shows an example of compilation detecting an inconsistent policy rule.

B.1 Inconsistent PLA

This PLA is inconsistent. “Geva” and “gpatz” refer to the same endpoint and, similarly, “Alex” and “acolvin” represent the same endpoint, but the policy rules concerning communications between “Alex” and “Geva” and “acolvin” and “gpatz” require that different algorithms be utilized to secure the communication. However, since the communications are indistinguishable at the concrete (IPsec) level, the two policy rules represent a conflict.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "pla11.dtd">

<!-- Autogenerated from PLACID source -->

<PLA>
    <Head>
        <Coalition name="Example_Coalition">
            <Partner name="Alexstan" />
            <Partner name="Gevania" />
        </Coalition>
        <Owner name="Gevania" />
        <Scope partners="Alexstan Gevania" />
    </Head>
    <GlobalDict>
        <Binding name="Alex" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.1.2.3" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="Alex" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSEndpoint type="remote">
                        <IPAddress value="10.1.2.3" />
                    </TLSEndpoint>
                    <TLSVersion value="3.0" />
                </TLSSelector>
            </Value>
        </Binding>
        <Binding name="acolvin" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.1.2.3" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="acolvin" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSVersion value="3.0" />
                    <TLSUserID value="acolvin" />
                </TLSSelector>
            </Value>
        </Binding>
    </GlobalDict>
    <PolicyAgreement pla_version="42" this_partner="Gevania">
        <Binding name="Geva" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.100.102.123" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="Geva" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSEndpoint type="local">
                        <IPAddress value="10.100.103.123" />
                    </TLSEndpoint>
                    <TLSVersion value="3.0" />
                </TLSSelector>
            </Value>
        </Binding>
        <Binding name="gpatz" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.100.102.123" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="gpatz" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSVersion value="3.0" />
                    <TLSUserID value="gpatz" />
                </TLSSelector>
            </Value>
        </Binding>
        <PolicySet interp="conjunct">
            <PolicyRule>
                <Condition>
                    <What>
                        <Name name="Alex" />
                    </What>
                    <What>
                        <Name name="Geva" />
                    </What>
                </Condition>
                <Action>
                    <ActionElement>
                        <DataConfidentiality>
                            <Name name="strong" />
                        </DataConfidentiality>
                    </ActionElement>
                </Action>
            </PolicyRule>
            <PolicyRule>
                <Condition>
                    <What>
                        <Name name="acolvin" />
                    </What>
                    <What>
                        <Name name="gpatz" />
                    </What>
                </Condition>
                <Action>
                    <ActionElement>
                        <DataConfidentiality>
                            <Name name="high" />
                        </DataConfidentiality>
                    </ActionElement>
                </Action>
            </PolicyRule>
            <Binding type="service_mechanism_mapping" name="strong">
                <Value>
                    <Encipherment type="reversible_symmetric">
                        <Name name="strong_crypto" />
                    </Encipherment>
                </Value>
            </Binding>
            <Binding type="service_mechanism_mapping" name="high">
                <Value>
                    <Encipherment type="reversible_symmetric">
                        <Name name="high_crypto" />
                    </Encipherment>
                </Value>
            </Binding>
            <Binding name="high_crypto" context="IPsec" type="mechanism_context_params" >
                <Value>
                    <EspProposal>
                        <IpsecCipher value="Blowfish" />
                    </EspProposal>
                </Value>
            </Binding>
            <Binding name="strong_crypto" context="IPsec" type="mechanism_context_params" >
                <Value>
                    <EspProposal>
                        <IpsecCipher value="Idea3" />
                        <IpsecCipher value="Des3" />
                    </EspProposal>
                </Value>
            </Binding>
        </PolicySet>
    </PolicyAgreement>
</PLA>
```

B.2 Error Output

The error output from the compiler indicates where the inconsistency was detected so the administrator can correct the problem.

```
bash-2.03$ plamodel < ex2a.xml | placheck
inconsistent
*       RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
*       RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
.
sets 1  conds 1 acts 1  exprs 6 alts 26 confs 5 terms 3
check failed
```

The ouput specifies the policy rules that are inconsistent by their xpaths. While this output is not directly useful for the administrator to read, it can be used by a GUI to find and display the inconsistent rules.

B.3 Consistent PLA

This policy shows one way an administrator might correct the inconsistency in the previous PLA. Here we added two consistent concrete mechanism bindings in the TLS context with the same binding names as their IPsec counterparts. Now, while the IPsec context is still inconsistent, the PLA is consistent since the two rules are consistent in the TLS context.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "plal1.dtd">

<!-- Autogenerated from PLACID source -->

<PLA>
    <Head>
        <Coalition name="Example_Coalition">
            <Partner name="Alexstan" />
            <Partner name="Gevania" />
        </Coalition>
        <Owner name="Gevania" />
        <Scope partners="Alexstan Gevania" />
    </Head>
    <GlobalDict>
        <Binding name="Alex" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.1.2.3" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="Alex" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSEndpoint type="remote">
                        <IPAddress value="10.1.2.3" />
                    </TLSEndpoint>
                    <TLSVersion value="3.0" />
                </TLSSelector>
            </Value>
        </Binding>
        <Binding name="acolvin" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.1.2.3" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="acolvin" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSVersion value="3.0" />
                    <TLSUserID value="acolvin" />
                </TLSSelector>
            </Value>
        </Binding>
    </GlobalDict>
    <PolicyAgreement pla_version="42" this_partner="Gevania">
        <Binding name="Geva" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.100.102.123" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="Geva" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSEndpoint type="local">
                        <IPAddress value="10.100.103.123" />
                    </TLSEndpoint>
                    <TLSVersion value="3.0" />
                </TLSSelector>
            </Value>
        </Binding>
        <Binding name="gpatz" context="IPsec" type="asset_context_params" >
            <Value>
                <IPsecSelector>
                    <IPAddress value="10.100.102.123" />
                </IPsecSelector>
            </Value>
        </Binding>
        <Binding name="gpatz" context="TLS" type="asset_context_params" >
            <Value>
                <TLSSelector>
                    <TLSVersion value="3.0" />
                    <TLSUserID value="gpatz" />
                </TLSSelector>
            </Value>
        </Binding>
        <PolicySet interp="conjunct">
            <PolicyRule>
                <Condition>
                    <What>
                        <Name name="Alex" />
                    </What>
                    <What>
                        <Name name="Geva" />
                    </What>
                </Condition>
                <Action>
                    <ActionElement>
                        <DataConfidentiality>
                            <Name name="strong" />
                        </DataConfidentiality>
                    </ActionElement>
                </Action>
            </PolicyRule>
            <PolicyRule>
                <Condition>
                    <What>
                        <Name name="acolvin" />
                    </What>
                    <What>
                        <Name name="gpatz" />
                    </What>
                </Condition>
                <Action>
                    <ActionElement>
                        <DataConfidentiality>
                            <Name name="high" />
                        </DataConfidentiality>
                    </ActionElement>
                </Action>
            </PolicyRule>
            <Binding type="service_mechanism_mapping" name="strong">
                <Value>
                    <Encipherment type="reversible_symmetric">
                        <Name name="strong_crypto" />
                    </Encipherment>
                </Value>
            </Binding>
            <Binding type="service_mechanism_mapping" name="high">
                <Value>
                    <Encipherment type="reversible_symmetric">
                        <Name name="high_crypto" />
                    </Encipherment>
                </Value>
            </Binding>
            <Binding name="high_crypto" context="TLS" type="mechanism_context_params" >
                <Value>
                    <TLSAction>
                        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
                        <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
                    </TLSAction>
                </Value>
            </Binding>
            <Binding name="strong_crypto" context="TLS" type="mechanism_context_params" >
                <Value>
                    <TLSAction>
                        <TLSCipherAlg cipher="3des" keylength="112" block="true" />
                        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
                    </TLSAction>
                </Value>
            </Binding>
            <Binding name="high_crypto" context="IPsec" type="mechanism_context_params" >
                <Value>
                    <EspProposal>
                        <IpsecCipher value="Blowfish" />
                    </EspProposal>
                </Value>
            </Binding>
            <Binding name="strong_crypto" context="IPsec" type="mechanism_context_params" >
                <Value>
                    <EspProposal>
                        <IpsecCipher value="Idea3" />
                        <IpsecCipher value="Des3" />
                    </EspProposal>
                </Value>
            </Binding>
        </PolicySet>
    </PolicyAgreement>
</PLA>
```

C Resolution

This appendix shows an abbreviated example of resolution. In the interest of space, only a couple of the PLAs that are part of the resolution are included here. The full set of PLAs that are part of this resolution can be found as part of the MSME release in plal-examples/bigtest.

Additionally, we will start by showing the binding of a set of bindings to a set of abstract policy rules, which is part of the compilation process.

Please note that white space has been altered in some instances to produce more readable output, however the substance or meaning of the output has not been modified.

C.1 Coalition Policies

The example described in this section consists of ten coalition partners. The PLAs contain a set of policies that are described by the following table:

Ptnr	A	B	C	D	E	F	G	H	I	J	MC
A			H-H				H-A				X
B			H-H						A-A		X
C	H-H	H-H		H-H	H-H	H-H	H-H	H-H	H-H	H-H G-G	X
D			H-H		H-A						X
E				A-H		H-H		A-A			X
F					H-H		G-G				X
G	A-H		H-H			G-G					X
H	G-A		H-H		A-A						X
I		A-A	H-H								X
J			H-H G-G								X

The rows in this table represent the PLAs of the partners listed with each row. Any filled cell indicates that the PLA contains a policy rule between the assets of that partner and the partner at the intersecting column. The intersection contains two letters indicating the assets that the rule covers, the first belonging to the partner listed in the row, the second the partner in the column. An H indicates it's a "host", an A is an "agent," and a G is a "gateway." The final column represents "MissionCommand," which is controlled by partner A. An X in the column indicates that the partner has a rule allowing its hosts to communicate with "MissionCommand." Partner A has a policy that allows "MissionCommand" to communicate with all partners' hosts.

C.2 Partner A: Abstract Rules

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "plal1.dtd">

<PLA>

<Head>
  <Coalition name="secret_mission">
    <Partner name="partner_A"/>
    <Partner name="partner_B"/>
    <Partner name="partner_C"/>
    <Partner name="partner_D"/>
    <Partner name="partner_E"/>
    <Partner name="partner_F"/>
    <Partner name="partner_G"/>
    <Partner name="partner_H"/>
    <Partner name="partner_I"/>
    <Partner name="partner_J"/>
  </Coalition>

  <Owner name="partner_A"/>

  <Scope partners="partner_A partner_B partner_C partner_D
        partner_E partner_F partner_G partner_H partner_I partner_J" />
</Head>

<GlobalDict>

    <Declaration name="MissionCommand" owner="partner_A"/>
    <Declaration name="A_hosts" owner="partner_A"/>
    <Declaration name="A_agents" owner="partner_A"/>
    <Declaration name="A_gateways" owner="partner_A"/>

    <Declaration name="B_hosts" owner="partner_B"/>
    <Declaration name="B_agents" owner="partner_B"/>
    <Declaration name="B_gateways" owner="partner_B"/>

    <Declaration name="C_hosts" owner="partner_C"/>
    <Declaration name="C_agents" owner="partner_C"/>
    <Declaration name="C_gateways" owner="partner_C"/>

    <Declaration name="D_hosts" owner="partner_D"/>
    <Declaration name="D_agents" owner="partner_D"/>
    <Declaration name="D_gateways" owner="partner_D"/>

    <Declaration name="E_hosts" owner="partner_E"/>
    <Declaration name="E_agents" owner="partner_E"/>
    <Declaration name="E_gateways" owner="partner_E"/>

    <Declaration name="F_hosts" owner="partner_F"/>
    <Declaration name="F_agents" owner="partner_F"/>
    <Declaration name="F_gateways" owner="partner_F"/>

    <Declaration name="G_hosts" owner="partner_G"/>
    <Declaration name="G_agents" owner="partner_G"/>
    <Declaration name="G_gateways" owner="partner_G"/>

    <Declaration name="H_hosts" owner="partner_H"/>
    <Declaration name="H_agents" owner="partner_H"/>
    <Declaration name="H_gateways" owner="partner_H"/>

    <Declaration name="I_hosts" owner="partner_I"/>
    <Declaration name="I_agents" owner="partner_I"/>
    <Declaration name="I_gateways" owner="partner_I"/>

    <Declaration name="J_hosts" owner="partner_J"/>
    <Declaration name="J_agents" owner="partner_J"/>
    <Declaration name="J_gateways" owner="partner_J"/>

    <Declaration name="AllHosts" owner="partner_A"/>
     <Binding name="AllHosts" type="asset_composition">
      <Value>
          <Name name="A_hosts"/>
          <Name name="B_hosts"/>
          <Name name="C_hosts"/>
          <Name name="D_hosts"/>
          <Name name="E_hosts"/>
          <Name name="F_hosts"/>
          <Name name="G_hosts"/>
          <Name name="H_hosts"/>
          <Name name="I_hosts"/>
          <Name name="J_hosts"/>
      </Value>
    </Binding>

</GlobalDict>

<PolicyAgreement pla_version="1" this_partner="partner_A">

    <PolicySet interp="conjunct">

      <PolicyRule>
        <Condition>
          <What><Name name="MissionCommand"/></What>
          <What><Name name="AllHosts"/></What>
          <When><Name name="AMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Astrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Astrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="A_hosts"/></What>
          <What><Name name="C_hosts"/></What>
          <When><Name name="AMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Astrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Astrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="A_hosts"/></What>
          <What><Name name="G_agents"/></What>
          <When><Name name="AMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Astrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Astrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

    </PolicySet>

 </PolicyAgreement>

</PLA>
```

C.3 Partner A: Binding Library

```
<xml>

    <Binding name="AMissionTime" type="time">
      <Value>
        <TimePeriod>
          <TimeRange value="20020101T050000/20040630T050000" />
        </TimePeriod>
      </Value>
    </Binding>

    <Binding name="Astrong_cipher" type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="Astrong_cipher_mech"/>
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="Astrong_auth" type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="Astrong_auth_mech"/>
        </AuthenticationExchange>
      </Value>
    </Binding>

    <!-- IPsec Bindings -->

    <Binding name="MissionCommand" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.0.0.0-10.0.255.255"/>
          <Port value="22"/>
          <Port value="25"/>
          <Port value="443"/>
          <Port value="500"/>
          <Protocol value="tcp"/>
          <Protocol value="udp"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="A_hosts" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.1.0-10.1.200.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="A_agents" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.201.0-10.1.255.255"/>
          <Port value="22"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="A_gateways" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.0.0-10.1.0.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="Astrong_cipher_mech" type="mechanism_context_params"
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="Blowfish" />
            <IpsecCipher value="Des3" />
            <IpsecCipher value="Idea3" />
            <IpsecCipher value="Rc5" />
            <IpsecCipher value="Rfc1829-iv64" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <Binding name="Astrong_auth_mech" type="mechanism_context_params"
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="AnyAndNull" />
            <IpsecIntegrity value="HmacMd5" />
            <IpsecIntegrity value="HmacSha1" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <!-- TLS Bindings -->

    <Binding name="A_hosts" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.1.0-10.1.200.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="A_agents" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.201.0-10.1.255.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="A_gateways" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.0.0-10.1.0.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
```

```
      </Value>
    </Binding>

    <Binding name="Astrong_cipher_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
          <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
          <TLSCipherAlg cipher="idea" keylength="128" block="true" />
          <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>

    <Binding name="Astrong_auth_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSMacAlg value="sha" />
      </Value>
    </Binding>

</xml>
```

C.4 Partner A: PLA

This PLA was created by binding the above binding library to the set of abstract policies above.

```
<?xml version="1.0" ?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_A" />
      <Partner name="partner_B" />
      <Partner name="partner_C" />
      <Partner name="partner_D" />
      <Partner name="partner_E" />
      <Partner name="partner_F" />
      <Partner name="partner_G" />
      <Partner name="partner_H" />
      <Partner name="partner_I" />
      <Partner name="partner_J" />
    </Coalition>

    <Owner name="partner_A" />

    <Scope partners="partner_A partner_B partner_C partner_D partner_E
          partner_F partner_G partner_H partner_I partner_J" />
  </Head>

  <GlobalDict>
    <Declaration name="MissionCommand" owner="partner_A" />
    <Declaration name="A_hosts" owner="partner_A" />
    <Declaration name="A_agents" owner="partner_A" />
    <Declaration name="A_gateways" owner="partner_A" />
    <Declaration name="B_hosts" owner="partner_B" />
    <Declaration name="B_agents" owner="partner_B" />
    <Declaration name="B_gateways" owner="partner_B" />
    <Declaration name="C_hosts" owner="partner_C" />
    <Declaration name="C_agents" owner="partner_C" />
    <Declaration name="C_gateways" owner="partner_C" />
    <Declaration name="D_hosts" owner="partner_D" />
    <Declaration name="D_agents" owner="partner_D" />
    <Declaration name="D_gateways" owner="partner_D" />
    <Declaration name="E_hosts" owner="partner_E" />
    <Declaration name="E_agents" owner="partner_E" />
    <Declaration name="E_gateways" owner="partner_E" />
    <Declaration name="F_hosts" owner="partner_F" />
    <Declaration name="F_agents" owner="partner_F" />
    <Declaration name="F_gateways" owner="partner_F" />
    <Declaration name="G_hosts" owner="partner_G" />
    <Declaration name="G_agents" owner="partner_G" />
    <Declaration name="G_gateways" owner="partner_G" />
    <Declaration name="H_hosts" owner="partner_H" />
    <Declaration name="H_agents" owner="partner_H" />
    <Declaration name="H_gateways" owner="partner_H" />
    <Declaration name="I_hosts" owner="partner_I" />
    <Declaration name="I_agents" owner="partner_I" />
    <Declaration name="I_gateways" owner="partner_I" />
    <Declaration name="J_hosts" owner="partner_J" />
    <Declaration name="J_agents" owner="partner_J" />
    <Declaration name="J_gateways" owner="partner_J" />
    <Declaration name="AllHosts" owner="partner_A" />

    <Binding name="MissionCommand" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.0.0.0-10.0.255.255" />
          <Port value="22" />
          <Port value="25" />
          <Port value="443" />
          <Port value="500" />
          <Protocol value="tcp" />
          <Protocol value="udp" />
        </IPsecSelector>
```

```
      </Value>
    </Binding>

    <Binding name="A_hosts" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.1.0-10.1.200.255" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="A_hosts" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.1.0-10.1.200.255" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="A_agents" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.201.0-10.1.255.255" />
          <Port value="22" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="A_agents" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.201.0-10.1.255.255" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="A_gateways" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.1.0.0-10.1.0.255" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="A_gateways" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.1.0.0-10.1.0.255" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="AllHosts" type="asset_composition">
      <Value>
```

```
        <Name name="A_hosts" />
        <Name name="B_hosts" />
        <Name name="C_hosts" />
        <Name name="D_hosts" />
        <Name name="E_hosts" />
        <Name name="F_hosts" />
        <Name name="G_hosts" />
        <Name name="H_hosts" />
        <Name name="I_hosts" />
        <Name name="J_hosts" />
      </Value>
    </Binding>
  </GlobalDict>

  <PolicyAgreement pla_version="1" this_partner="partner_A">
    <PolicySet interp="conjunct">
      <PolicyRule>
        <Condition>
          <What>
            <Name name="MissionCommand" />
          </What>
          <What>
            <Name name="AllHosts" />
          </What>
          <When>
            <Name name="AMissionTime-1" />
          </When>
        </Condition>

        <Action>
          <ActionElement>
            <Authentication type="data_origin">
              <Name name="Astrong_auth-2" />
            </Authentication>
          </ActionElement>
          <ActionElement>
            <DataConfidentiality>
              <Name name="Astrong_cipher-3" />
            </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What>
            <Name name="A_hosts" />
          </What>
          <What>
            <Name name="C_hosts" />
          </What>
          <When>
            <Name name="AMissionTime-1" />
          </When>
        </Condition>

        <Action>
          <ActionElement>
            <Authentication type="data_origin">
              <Name name="Astrong_auth-2" />
            </Authentication>
          </ActionElement>
          <ActionElement>
            <DataConfidentiality>
              <Name name="Astrong_cipher-3" />
            </DataConfidentiality>
          </ActionElement>
        </Action>
    </PolicyRule>

      <PolicyRule>
        <Condition>
          <What>
            <Name name="A_hosts" />
          </What>
          <What>
            <Name name="G_agents" />
          </What>
          <When>
            <Name name="AMissionTime-1" />
          </When>
        </Condition>

        <Action>
          <ActionElement>
            <Authentication type="data_origin">
```

```
              <Name name="Astrong_auth-2" />
            </Authentication>
          </ActionElement>
          <ActionElement>
            <DataConfidentiality>
              <Name name="Astrong_cipher-3" />
            </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>
    </PolicySet>

    <Binding name="AMissionTime-1" type="time">
      <Value>
        <TimePeriod>
          <TimeRange value="20020101T050000/20040630T050000" />
        </TimePeriod>
      </Value>
    </Binding>

    <Binding name="Astrong_auth-2"
    type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="Astrong_auth_mech-4" />
        </AuthenticationExchange>
      </Value>
    </Binding>

    <Binding name="Astrong_cipher-3"
    type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="Astrong_cipher_mech-5" />
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="Astrong_auth_mech-4"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="AnyAndNull" />
          <IpsecIntegrity value="HmacMd5" />
          <IpsecIntegrity value="HmacSha1" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="Astrong_auth_mech-4"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding name="Astrong_cipher_mech-5"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="Blowfish" />
          <IpsecCipher value="Des3" />
          <IpsecCipher value="Idea3" />
          <IpsecCipher value="Rc5" />
          <IpsecCipher value="Rfc1829-iv64" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="Astrong_cipher_mech-5"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
        <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
        <TLSCipherAlg cipher="idea" keylength="128" block="true" />
        <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>
  </PolicyAgreement>
</PLA>
```

C.5 Partner C: PLA

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "plal1.dtd">

<PLA>

<Head>
  <Coalition name="secret_mission">
```

```
    <Partner name="partner_A"/>
    <Partner name="partner_B"/>
    <Partner name="partner_C"/>
    <Partner name="partner_D"/>
    <Partner name="partner_E"/>
    <Partner name="partner_F"/>
    <Partner name="partner_G"/>
    <Partner name="partner_H"/>
    <Partner name="partner_I"/>
    <Partner name="partner_J"/>
  </Coalition>

  <Owner name="partner_C"/>

  <Scope partners="partner_A partner_B partner_C partner_D partner_E
                   partner_F partner_G partner_H partner_I partner_J" />
</Head>

<GlobalDict>

    <Declaration name="MissionCommand" owner="partner_A"/>
    <Declaration name="A_hosts" owner="partner_A"/>
    <Declaration name="A_agents" owner="partner_A"/>
    <Declaration name="A_gateways" owner="partner_A"/>

    <Declaration name="B_hosts" owner="partner_B"/>
    <Declaration name="B_agents" owner="partner_B"/>
    <Declaration name="B_gateways" owner="partner_B"/>

    <Declaration name="C_hosts" owner="partner_C"/>
    <Declaration name="C_agents" owner="partner_C"/>
    <Declaration name="C_gateways" owner="partner_C"/>

    <Declaration name="D_hosts" owner="partner_D"/>
    <Declaration name="D_agents" owner="partner_D"/>
    <Declaration name="D_gateways" owner="partner_D"/>

    <Declaration name="E_hosts" owner="partner_E"/>
    <Declaration name="E_agents" owner="partner_E"/>
    <Declaration name="E_gateways" owner="partner_E"/>

    <Declaration name="F_hosts" owner="partner_F"/>
    <Declaration name="F_agents" owner="partner_F"/>
    <Declaration name="F_gateways" owner="partner_F"/>

    <Declaration name="G_hosts" owner="partner_G"/>
    <Declaration name="G_agents" owner="partner_G"/>
    <Declaration name="G_gateways" owner="partner_G"/>

    <Declaration name="H_hosts" owner="partner_H"/>
    <Declaration name="H_agents" owner="partner_H"/>
    <Declaration name="H_gateways" owner="partner_H"/>

    <Declaration name="I_hosts" owner="partner_I"/>
    <Declaration name="I_agents" owner="partner_I"/>
    <Declaration name="I_gateways" owner="partner_I"/>

    <Declaration name="J_hosts" owner="partner_J"/>
    <Declaration name="J_agents" owner="partner_J"/>
    <Declaration name="J_gateways" owner="partner_J"/>

    <Declaration name="AllHosts" owner="partner_A"/>

</GlobalDict>

<PolicyAgreement pla_version="2" this_partner="partner_C">

    <PolicySet interp="conjunct">

      <PolicyRule>
        <Condition>
          <What><Name name="MissionCommand"/></What>
          <What><Name name="C_hosts"/></What>
          <When><Name name="CMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Cstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Cstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="C_hosts"/></What>
          <What><Name name="COtherHosts"/></What>
          <When><Name name="CMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Cstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Cstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="C_gateways"/></What>
          <What><Name name="J_gateways"/></What>
          <When><Name name="CMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Cstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Cstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

    </PolicySet>

     <Binding name="COtherHosts" type="asset_composition">
     <Value>
         <Name name="A_hosts"/>
         <Name name="B_hosts"/>
         <Name name="D_hosts"/>
         <Name name="E_hosts"/>
         <Name name="F_hosts"/>
         <Name name="G_hosts"/>
         <Name name="H_hosts"/>
         <Name name="I_hosts"/>
         <Name name="J_hosts"/>
     </Value>
   </Binding>

   <Binding name="CMissionTime" type="time">
      <Value>
        <TimePeriod>
          <TimeRange value="20020101T050000/20040630T090000" />
        </TimePeriod>
      </Value>
    </Binding>

    <Binding name="Cstrong_cipher" type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="Cstrong_cipher_mech"/>
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="Cstrong_auth" type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="Cstrong_auth_mech"/>
        </AuthenticationExchange>
      </Value>
    </Binding>

    <!-- IPsec Bindings -->

    <Binding name="C_hosts" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.3.1.0-10.3.200.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="C_agents" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.3.201.0-10.3.255.255"/>
          <Port value="22"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="C_gateways" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.3.0.0-10.3.0.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="Cstrong_cipher_mech" type="mechanism_context_params"
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="Blowfish" />
            <IpsecCipher value="Des3" />
            <IpsecCipher value="Idea3" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <Binding name="Cstrong_auth_mech" type="mechanism_context_params"
```

```
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="AnyAndNull" />
            <IpsecIntegrity value="HmacMd5" />
            <IpsecIntegrity value="HmacSha1" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <!-- TLS Bindings -->

    <Binding name="C_hosts" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.3.1.0-10.3.200.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="C_agents" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.3.201.0-10.3.255.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="C_gateways" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.3.0.0-10.3.0.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="Cstrong_cipher_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
          <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
          <TLSCipherAlg cipher="idea" keylength="128" block="true" />
          <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>

    <Binding name="Cstrong_auth_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSMacAlg value="sha" />
      </Value>
    </Binding>

 </PolicyAgreement>

</PLA>
```

C.6 Partner G: PLA

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN" "pla11.dtd">

<PLA>

<Head>
  <Coalition name="secret_mission">
    <Partner name="partner_A"/>
    <Partner name="partner_B"/>
    <Partner name="partner_C"/>
    <Partner name="partner_D"/>
    <Partner name="partner_E"/>
    <Partner name="partner_F"/>
    <Partner name="partner_G"/>
    <Partner name="partner_H"/>
    <Partner name="partner_I"/>
    <Partner name="partner_J"/>
  </Coalition>

  <Owner name="partner_G"/>

  <Scope partners="partner_A partner_B partner_C partner_D partner_E
                  partner_F partner_G partner_H partner_I partner_J" />
</Head>

<GlobalDict>

    <Declaration name="MissionCommand" owner="partner_A"/>
    <Declaration name="A_hosts" owner="partner_A"/>
    <Declaration name="A_agents" owner="partner_A"/>
    <Declaration name="A_gateways" owner="partner_A"/>

    <Declaration name="B_hosts" owner="partner_B"/>
    <Declaration name="B_agents" owner="partner_B"/>
    <Declaration name="B_gateways" owner="partner_B"/>

    <Declaration name="C_hosts" owner="partner_C"/>
    <Declaration name="C_agents" owner="partner_C"/>
    <Declaration name="C_gateways" owner="partner_C"/>

    <Declaration name="D_hosts" owner="partner_D"/>
    <Declaration name="D_agents" owner="partner_D"/>
    <Declaration name="D_gateways" owner="partner_D"/>

    <Declaration name="E_hosts" owner="partner_E"/>
    <Declaration name="E_agents" owner="partner_E"/>
    <Declaration name="E_gateways" owner="partner_E"/>

    <Declaration name="F_hosts" owner="partner_F"/>
    <Declaration name="F_agents" owner="partner_F"/>
    <Declaration name="F_gateways" owner="partner_F"/>

    <Declaration name="G_hosts" owner="partner_G"/>
    <Declaration name="G_agents" owner="partner_G"/>
    <Declaration name="G_gateways" owner="partner_G"/>

    <Declaration name="H_hosts" owner="partner_H"/>
    <Declaration name="H_agents" owner="partner_H"/>
    <Declaration name="H_gateways" owner="partner_H"/>

    <Declaration name="I_hosts" owner="partner_I"/>
    <Declaration name="I_agents" owner="partner_I"/>
    <Declaration name="I_gateways" owner="partner_I"/>

    <Declaration name="J_hosts" owner="partner_J"/>
    <Declaration name="J_agents" owner="partner_J"/>
    <Declaration name="J_gateways" owner="partner_J"/>

    <Declaration name="AllHosts" owner="partner_A"/>

</GlobalDict>

<PolicyAgreement pla_version="1" this_partner="partner_G">

    <PolicySet interp="conjunct">

      <PolicyRule>
        <Condition>
          <What><Name name="MissionCommand"/></What>
          <What><Name name="G_hosts"/></What>
          <When><Name name="GMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Gstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Gstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="G_hosts"/></What>
          <What><Name name="C_hosts"/></What>
          <When><Name name="GMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Gstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Gstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="G_agents"/></What>
          <What><Name name="A_hosts"/></What>
          <When><Name name="GMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Gstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Gstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

      <PolicyRule>
        <Condition>
          <What><Name name="G_gateways"/></What>
          <What><Name name="F_gateways"/></What>
          <When><Name name="GMissionTime"/></When>
        </Condition>
        <Action>
          <ActionElement>
             <Authentication type="data_origin">
               <Name name="Gstrong_auth"/>
             </Authentication>
          </ActionElement>
          <ActionElement>
             <DataConfidentiality>
               <Name name="Gstrong_cipher"/>
             </DataConfidentiality>
          </ActionElement>
        </Action>
      </PolicyRule>

    </PolicySet>

    <Binding name="GMissionTime" type="time">
      <Value>
        <TimePeriod>
          <TimeRange value="20020101T050000/20040630T050000" />
        </TimePeriod>
      </Value>
    </Binding>

    <Binding name="Gstrong_cipher" type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="Gstrong_cipher_mech"/>
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="Gstrong_auth" type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="Gstrong_auth_mech"/>
        </AuthenticationExchange>
      </Value>
    </Binding>

    <!-- IPsec Bindings -->

    <Binding name="G_hosts" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.7.1.0-10.7.200.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="G_agents" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.7.201.0-10.7.255.255"/>
          <Port value="22"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="G_gateways" type="asset_context_params" context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.7.0.0-10.7.0.255"/>
        </IPsecSelector>
      </Value>
     </Binding>

    <Binding name="Gstrong_cipher_mech" type="mechanism_context_params"
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="Blowfish" />
            <IpsecCipher value="Des3" />
            <IpsecCipher value="Idea3" />
            <IpsecCipher value="Rc5" />
            <IpsecCipher value="Rfc1829-iv64" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <Binding name="Gstrong_auth_mech" type="mechanism_context_params"
             context="IPsec">
      <Value>
          <EspProposal>
            <IpsecCipher value="AnyAndNull" />
            <IpsecIntegrity value="HmacMd5" />
            <IpsecIntegrity value="HmacSha1" />
            <IpsecExpiry type="seconds" value="0-600" />
            <IpsecType value="tunnel" />
          </EspProposal>
      </Value>
    </Binding>

    <!-- TLS Bindings -->

    <Binding name="G_hosts" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.7.1.0-10.7.200.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="G_agents" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.7.201.0-10.7.255.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="G_gateways" type="asset_context_params" context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.7.0.0-10.7.0.255"/>
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="Gstrong_cipher_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
          <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
          <TLSCipherAlg cipher="idea" keylength="128" block="true" />
          <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>

    <Binding name="Gstrong_auth_mech" type="mechanism_context_params"
             context="TLS">
      <Value>
          <TLSMacAlg value="sha" />
      </Value>
    </Binding>

 </PolicyAgreement>

</PLA>
```

C.7 RPLA

This RPLA is the result of the resolution of the ten PLA example.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE PLA PUBLIC "-//IETF//DTD RFCxxxx SAL v0.2//EN"
"plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_A" />
      <Partner name="partner_B" />
      <Partner name="partner_C" />
      <Partner name="partner_D" />
      <Partner name="partner_E" />
      <Partner name="partner_F" />
      <Partner name="partner_G" />
      <Partner name="partner_H" />
      <Partner name="partner_I" />
      <Partner name="partner_J" />
    </Coalition>

    <Owner name="partner_D" />

    <Scope
    partners="partner_A partner_B partner_C partner_D partner_E
              partner_F partner_G partner_H partner_I partner_J" />
  </Head>

  <ResolvedPolicyAgreement rpla_version="0" resolver_identity="partner_D">
    <ComponentPLA partner="partner_A" version="1" />
    <ComponentPLA partner="partner_B" version="2" />
    <ComponentPLA partner="partner_C" version="2" />
    <ComponentPLA partner="partner_D" version="2" />
    <ComponentPLA partner="partner_E" version="2" />
    <ComponentPLA partner="partner_F" version="2" />
    <ComponentPLA partner="partner_G" version="1" />
    <ComponentPLA partner="partner_H" version="1" />
    <ComponentPLA partner="partner_I" version="2" />
    <ComponentPLA partner="partner_J" version="2" />

    <PolicySet interp="disjunct">
      <PolicySet interp="conjunct">
        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="MissionCommand" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_D-bind188" />
            </What>
            <When>
              <Name name="partner_D-bind187" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind192" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind190" />
              </DataConfidentiality>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="MissionCommand" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_D-bind194" />
            </What>
            <When>
              <Name name="partner_D-bind193" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind198" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind196" />
              </DataConfidentiality>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="B_agents" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="I_agents" />
            </What>
            <When>
              <Name name="partner_D-bind199" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind204" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind202" />
              </DataConfidentiality>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="C_hosts" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_D-bind209" />
            </What>
            <When>
              <Name name="partner_D-bind207" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind213" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind211" />
              </DataConfidentiality>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="C_hosts" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_D-bind214" />
            </What>
            <When>
              <Name name="partner_D-bind208" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind218" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind216" />
              </DataConfidentiality>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="C_gateways" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="J_gateways" />
            </What>
            <When>
              <Name name="partner_D-bind208" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_D-bind218" />
              </Authentication>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_D-bind216" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind95" />
    </What>
    <When>
      <Name name="partner_D-bind97" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind101" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind99" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind96" />
    </What>
    <When>
      <Name name="partner_D-bind102" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind106" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind104" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind108" />
    </What>
    <When>
      <Name name="partner_D-bind107" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind112" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind110" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind115" />
    </What>
    <When>
      <Name name="partner_D-bind114" />
    </When>
  </Condition>
```

```
  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind119" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind117" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="A_hosts" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="G_agents" />
    </What>
    <When>
      <Name name="partner_D-bind107" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind112" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind110" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="C_hosts" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind144" />
    </What>
    <When>
      <Name name="partner_D-bind140" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind148" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind146" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="C_hosts" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind149" />
    </What>
    <When>
      <Name name="partner_D-bind141" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind153" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind151" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
```

```
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="D_hosts" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="E_agents" />
    </What>
    <When>
      <Name name="partner_D-bind157" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind164" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind162" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind6" />
    </What>
    <When>
      <Name name="partner_D-bind26" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind30" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind28" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind33" />
    </What>
    <When>
      <Name name="partner_D-bind32" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind37" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind35" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind38" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="C_hosts" />
    </What>
    <When>
      <Name name="partner_D-bind26" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind30" />
      </Authentication>
```

```
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind28" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind41" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="C_hosts" />
    </What>
    <When>
      <Name name="partner_D-bind40" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind46" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind44" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="MissionCommand" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind1" />
    </What>
    <When>
      <Name name="partner_D-bind0" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind5" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind3" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="C_hosts" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_D-bind8" />
    </What>
    <When>
      <Name name="partner_D-bind7" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_D-bind12" />
      </Authentication>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_D-bind10" />
      </DataConfidentiality>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="E_agents" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="H_agents" />
```

```
        </What>
        <When>
          <Name name="partner_D-bind50" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin" choice="Required">
            <Name name="partner_D-bind54" />
          </Authentication>
        </ActionElement>
        <ActionElement>
          <DataConfidentiality type="connectionless"
          choice="Required">
            <Name name="partner_D-bind52" />
          </DataConfidentiality>
        </ActionElement>
      </Action>
    </PolicyRule>

    <PolicyRule>
      <Condition>
        <What direction="both" type="any" role="none">
          <Name name="F_gateways" />
        </What>
        <What direction="both" type="any" role="none">
          <Name name="G_gateways" />
        </What>
        <When>
          <Name name="partner_D-bind55" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin" choice="Required">
            <Name name="partner_D-bind60" />
          </Authentication>
        </ActionElement>
        <ActionElement>
          <DataConfidentiality type="connectionless"
          choice="Required">
            <Name name="partner_D-bind58" />
          </DataConfidentiality>
        </ActionElement>
      </Action>
    </PolicyRule>

    <PolicyRule>
      <Condition>
        <What direction="both" type="any" role="none">
          <Name name="E_hosts" />
        </What>
        <What direction="both" type="any" role="none">
          <Name name="F_hosts" />
        </What>
        <When>
          <Name name="partner_D-bind13" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin" choice="Required">
            <Name name="partner_D-bind17" />
          </Authentication>
        </ActionElement>
        <ActionElement>
          <DataConfidentiality type="connectionless"
          choice="Required">
            <Name name="partner_D-bind15" />
          </DataConfidentiality>
        </ActionElement>
      </Action>
    </PolicyRule>
  </PolicySet>
</PolicySet>

<Binding name="MissionCommand" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.0.0-10.0.255.255" />
      <Port value="22" />
      <Port value="25" />
      <Port value="443" />
      <Port value="500" />
      <Protocol value="tcp" />
      <Protocol value="udp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="A_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.1.1.0-10.1.200.255" />
    </IPsecSelector>
  </Value>
```

```
</Binding>

<Binding name="A_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.1.1.0-10.1.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="A_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.1.201.0-10.1.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="A_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.1.201.0-10.1.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="A_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.1.0.0-10.1.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="A_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.1.0.0-10.1.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="B_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.2.1.0-10.2.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="B_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.2.1.0-10.2.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="B_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.2.201.0-10.2.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="B_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.2.201.0-10.2.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="B_gateways" type="asset_context_params"
```

```
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.2.0.0-10.2.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="B_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.2.0.0-10.2.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="C_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.3.1.0-10.3.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="C_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.3.1.0-10.3.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="C_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.3.201.0-10.3.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="C_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.3.201.0-10.3.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="C_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.3.0.0-10.3.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="C_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.3.0.0-10.3.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="D_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.4.1.0-10.4.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="D_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.4.201.0-10.4.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="D_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.4.0.0-10.4.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="E_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.5.1.0-10.5.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="E_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.5.1.0-10.5.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="E_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.5.201.0-10.5.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="E_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.5.201.0-10.5.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="E_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.5.0.0-10.5.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="E_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.5.0.0-10.5.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="F_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.6.1.0-10.6.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="F_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.6.1.0-10.6.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="F_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.6.201.0-10.6.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="F_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.6.201.0-10.6.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="F_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.6.0.0-10.6.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="F_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.6.0.0-10.6.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="G_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.7.1.0-10.7.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="G_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.7.1.0-10.7.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="G_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.7.201.0-10.7.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="G_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.7.201.0-10.7.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="G_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.7.0.0-10.7.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="G_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.7.0.0-10.7.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="H_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.8.1.0-10.8.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="H_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.8.1.0-10.8.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="H_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.8.201.0-10.8.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="H_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.8.201.0-10.8.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="H_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.8.0.0-10.8.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="H_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.8.0.0-10.8.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="I_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.9.1.0-10.9.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="I_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.9.1.0-10.9.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="I_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.9.201.0-10.9.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="I_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
```

```
        <IPAddress value="10.9.201.0-10.9.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="I_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.9.0.0-10.9.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="I_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.9.0.0-10.9.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="J_hosts" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.10.1.0-10.10.200.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="J_hosts" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.10.1.0-10.10.200.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="J_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.10.201.0-10.10.255.255" />
      <Port value="22" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="J_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.10.201.0-10.10.255.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="J_gateways" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.10.0.0-10.10.0.255" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="J_gateways" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.10.0.0-10.10.0.255" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="AllHosts" type="asset_composition">
  <Value>
    <Name name="A_hosts" />
    <Name name="B_hosts" />
    <Name name="C_hosts" />
    <Name name="D_hosts" />
    <Name name="E_hosts" />
    <Name name="F_hosts" />
    <Name name="G_hosts" />
    <Name name="H_hosts" />
    <Name name="I_hosts" />
    <Name name="J_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind188">
  <Value>
    <Name name="I_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind188">
  <Value>
    <Name name="I_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind187">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind192">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind191" />
      <Name name="partner_D-bind191" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind190">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind189" />
      <Name name="partner_D-bind189" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind194">
  <Value>
    <Name name="J_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind194">
  <Value>
    <Name name="J_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind193">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind198">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind197" />
      <Name name="partner_D-bind197" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind196">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind195" />
      <Name name="partner_D-bind195" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind199">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind204">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind203" />
      <Name name="partner_D-bind203" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind202">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind201" />
      <Name name="partner_D-bind201" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind209">
  <Value>
    <Name name="I_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind209">
  <Value>
    <Name name="I_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind207">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind213">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind212" />
      <Name name="partner_D-bind212" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind211">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind210" />
      <Name name="partner_D-bind210" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind214">
  <Value>
    <Name name="J_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind214">
  <Value>
    <Name name="J_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind208">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind218">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind217" />
      <Name name="partner_D-bind217" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind216">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind215" />
      <Name name="partner_D-bind215" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind95">
  <Value>
    <Name name="E_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind95">
  <Value>
    <Name name="E_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind97">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind101">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind100" />
      <Name name="partner_D-bind100" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind99">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind98" />
      <Name name="partner_D-bind98" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind96">
  <Value>
    <Name name="F_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind96">
  <Value>
    <Name name="F_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind102">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind106">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind105" />
      <Name name="partner_D-bind105" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind104">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind103" />
      <Name name="partner_D-bind103" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind108">
  <Value>
    <Name name="G_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind108">
  <Value>
    <Name name="G_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind107">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind112">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind111" />
      <Name name="partner_D-bind111" />
    </AuthenticationExchange>
  </Value>
</Binding>
```

```
<Binding type="service_mechanism_mapping"
name="partner_D-bind110">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind109" />
      <Name name="partner_D-bind109" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind115">
  <Value>
    <Name name="H_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind115">
  <Value>
    <Name name="H_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind114">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind119">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind118" />
      <Name name="partner_D-bind118" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind117">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind116" />
      <Name name="partner_D-bind116" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind144">
  <Value>
    <Name name="G_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind144">
  <Value>
    <Name name="G_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind140">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind148">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind147" />
      <Name name="partner_D-bind147" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind146">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind145" />
      <Name name="partner_D-bind145" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind149">
  <Value>
    <Name name="H_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind149">
  <Value>
    <Name name="H_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind141">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind153">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind152" />
      <Name name="partner_D-bind152" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind151">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind150" />
      <Name name="partner_D-bind150" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind157">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind164">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind163" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind162">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind161" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind6">
  <Value>
    <Name name="C_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind6">
  <Value>
    <Name name="C_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind26">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind30">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind29" />
      <Name name="partner_D-bind29" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind28">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind27" />
      <Name name="partner_D-bind27" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind33">
  <Value>
    <Name name="D_hosts" />
  </Value>
</Binding>
```

```
<Binding type="time" name="partner_D-bind32">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind37">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind36" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind35">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind34" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_D-bind38">
  <Value>
    <Name name="A_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" context="TLS"
name="partner_D-bind38">
  <Value>
    <Name name="A_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_D-bind41">
  <Value>
    <Name name="B_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" context="TLS"
name="partner_D-bind41">
  <Value>
    <Name name="B_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind40">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind46">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind45" />
      <Name name="partner_D-bind45" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind44">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind43" />
      <Name name="partner_D-bind43" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind1">
  <Value>
    <Name name="B_hosts" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind1">
  <Value>
    <Name name="B_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind0">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind5">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind4" />

      <Name name="partner_D-bind4" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind3">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind2" />
      <Name name="partner_D-bind2" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_D-bind8">
  <Value>
    <Name name="D_hosts" />
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind7">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind12">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind11" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind10">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind9" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind50">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind54">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind53" />
      <Name name="partner_D-bind53" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind52">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind51" />
      <Name name="partner_D-bind51" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind55">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind60">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind59" />
      <Name name="partner_D-bind59" />
    </AuthenticationExchange>
  </Value>
</Binding>
```

```
<Binding type="service_mechanism_mapping"
name="partner_D-bind58">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind57" />
      <Name name="partner_D-bind57" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="time" name="partner_D-bind13">
  <Value>
    <TimePeriod>
      <TimeRange value="20020101T050000/20040630T050000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind17">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_D-bind16" />
      <Name name="partner_D-bind16" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_D-bind15">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_D-bind14" />
      <Name name="partner_D-bind14" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind191">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind191">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind189">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind189">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind197">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind197">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind195">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind195">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind203">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind203">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind201">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind201">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind212">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind212">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind210">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind210">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind217">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind217">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind215">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind215">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind100">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind100">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind98">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind98">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind105">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind105">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind103">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind103">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind111">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind111">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind109">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind109">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind118">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind118">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind116">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind116">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind147">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind147">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind145">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>
```

```
<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind145">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind152">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind152">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind150">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind150">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind163">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind161">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind29">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
```

```
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind29">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind27">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind27">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind36">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind34">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind45">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind45">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind43">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind43">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind4">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind4">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind2">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecCipher value="Rc5" not="false" />
      <IpsecCipher value="Rfc1829-iv64" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind2">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="des3" block="true" keylength="112">
    </TLSCipherAlg>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind11">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind9">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Blowfish" not="false" />
      <IpsecCipher value="Des3" not="false" />
      <IpsecCipher value="Idea3" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_D-bind53">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_D-bind53">
  <Value>
```

```
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_D-bind51">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_D-bind51">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_D-bind59">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacMd5" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_D-bind59">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_D-bind57">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_D-bind57">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_D-bind16">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacMd5" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_D-bind16">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_D-bind14">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_D-bind14">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>
  </ResolvedPolicyAgreement>
</PLA>
```

D Monitoring

This appendix shows some examples of errors that reconciliation can detect. These are taken from the tests directory in the MSME release.

More examples of tests can be found as part of the MSME release in plal-examples/reconciliation-tests.

D.1 PLA 1

A PLA for Partner 1:

```
<?xml version="1.0" ?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_1" />
      <Partner name="partner_2" />
    </Coalition>

    <Owner name="partner_1" />

    <Scope partners="partner_1 partner_2" />
  </Head>

  <GlobalDict>
    <Declaration name="P1_servers" owner="partner_1" />
    <Declaration name="P1_clients" owner="partner_1" />
    <Declaration name="P1_ca" owner="partner_1" />
    <Declaration name="P2_servers" owner="partner_2" />
    <Declaration name="P2_clients" owner="partner_2" />
    <Declaration name="P2_ca" owner="partner_2" />

    <Binding name="P1_servers" type="asset_composition">
      <Value>
        <Name name="P1_servers_80-1" />
        <Name name="P1_servers_443-2" />
    </Value>
  </Binding>

  <Binding name="P1_clients" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="10.100/16" />
        <Port value="any" />
        <Protocol value="tcp" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P1_clients" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="10.100/16" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
        <TLSRole value="client" />
      </TLSSelector>
    </Value>
  </Binding>

  <Binding name="P1_ca" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="10.0.10.32" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P1_ca" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.10.32" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
      </TLSSelector>
    </Value>
  </Binding>

  <Binding name="P1_servers_80-1" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="10.0.1.24" />
        <IPAddress value="10.0.3.164" />
        <IPAddress value="10.0.10.2" />
        <Port value="80" />
        <Protocol value="tcp" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P1_servers_80-1" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.1.24" />
        </TLSEndpoint>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.3.164" />
        </TLSEndpoint>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.10.2" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
        <TLSRole value="server" />
        <TLSService>
          <Port value="80" />
        </TLSService>
      </TLSSelector>
    </Value>
  </Binding>

  <Binding name="P1_servers_443-2" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="10.0.1.24" />
        <IPAddress value="10.0.3.164" />
        <IPAddress value="10.0.10.2" />
        <Port value="443" />
        <Protocol value="tcp" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P1_servers_443-2" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.1.24" />
        </TLSEndpoint>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.3.164" />
        </TLSEndpoint>
        <TLSEndpoint type="local">
          <IPAddress value="10.0.10.2" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
        <TLSRole value="server" />
        <TLSService>
          <Port value="443" />
        </TLSService>
      </TLSSelector>
    </Value>
  </Binding>
</GlobalDict>

<PolicyAgreement pla_version="1" this_partner="partner_1">
  <PolicySet interp="conjunct">
    <PolicyRule>
      <Condition>
        <What>
          <Name name="P1_clients" />
        </What>
        <What>
          <Name name="P2_servers" />
        </What>
        <When>
          <Name name="MissionTime-3" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin">
            <Name name="good_auth-4" />
          </Authentication>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>

        <ActionElement>
          <DataConfidentiality>
            <Name name="good_cipher-5" />
          </DataConfidentiality>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>
      </Action>
    </PolicyRule>

    <PolicyRule>
      <Condition>
        <What>
          <Name name="P2_clients" />
        </What>
        <What>
          <Name name="P1_servers_80-1" />
        </What>
        <When>
          <Name name="MissionTime-3" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin">
            <Name name="strong_auth-6" />
          </Authentication>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>

        <ActionElement>
          <DataConfidentiality>
            <Name name="strong_cipher-7" />
          </DataConfidentiality>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>
      </Action>
    </PolicyRule>
  </PolicySet>
```

```
    <Binding name="MissionTime-3" type="time">
      <Value>
        <TimePeriod>
          <TimeRange value="20010101T050000/THISANDFUTURE" />
        </TimePeriod>
      </Value>
    </Binding>

    <Binding name="good_auth-4" type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="good_auth_mech-8" />
        </AuthenticationExchange>
      </Value>
    </Binding>

    <Binding name="good_cipher-5" type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="good_cipher_mech-9" />
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="strong_auth-6" type="service_mechanism_mapping">
      <Value>
        <AuthenticationExchange>
          <Name name="strong_auth_mech-10" />
        </AuthenticationExchange>
      </Value>
    </Binding>

    <Binding name="strong_cipher-7"
    type="service_mechanism_mapping">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="strong_cipher_mech-11" />
        </Encipherment>
      </Value>
    </Binding>

    <Binding name="good_auth_mech-8"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="AnyAndNull" />
          <IpsecIntegrity value="Any" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="good_auth_mech-8"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSMacAlg value="md5" />
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding name="good_cipher_mech-9"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="Any" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="good_cipher_mech-9"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
        <TLSCipherAlg cipher="rc4" keylength="40" block="false" />
        <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
        <TLSCipherAlg cipher="rc2" keylength="40" block="true" />
        <TLSCipherAlg cipher="idea" keylength="128" block="true" />
        <TLSCipherAlg cipher="des" keylength="56" block="true" />
        <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>

    <Binding name="strong_auth_mech-10"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="AnyAndNull" />
          <IpsecIntegrity value="HmacMd5" />
          <IpsecIntegrity value="HmacSha1" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="strong_auth_mech-10"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding name="strong_cipher_mech-11"
    type="mechanism_context_params" context="IPsec">
      <Value>
        <EspProposal>
          <IpsecCipher value="Blowfish" />
          <IpsecCipher value="Des3" />
          <IpsecCipher value="Idea3" />
          <IpsecCipher value="Rc5" />
          <IpsecCipher value="Rfc1829-iv64" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding name="strong_cipher_mech-11"
    type="mechanism_context_params" context="TLS">
      <Value>
        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
        <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
        <TLSCipherAlg cipher="idea" keylength="128" block="true" />
        <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>
  </PolicyAgreement>
</PLA>
```

D.2 PLA 2

A PLA for Partner 2:

```
<?xml version="1.0" ?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_1" />
      <Partner name="partner_2" />
    </Coalition>

    <Owner name="partner_2" />

    <Scope partners="partner_1 partner_2" />
  </Head>

  <GlobalDict>
    <Declaration name="P1_servers" owner="partner_1" />
    <Declaration name="P1_clients" owner="partner_1" />
    <Declaration name="P1_ca" owner="partner_1" />
    <Declaration name="P2_servers" owner="partner_2" />
    <Declaration name="P2_clients" owner="partner_2" />
    <Declaration name="P2_ca" owner="partner_2" />
    <Binding name="P2_servers" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="192.168.4.64" />
          <IPAddress value="192.168.2.15" />
          <Port value="443" />
          <Port value="80" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P2_servers" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="192.168.4.64" />
          </TLSEndpoint>
          <TLSEndpoint type="local">
            <IPAddress value="192.168.2.15" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
          <TLSVersion value="2.0" />
          <TLSRole value="server" />
          <TLSService>
            <Port value="443" />
            <Port value="80" />
        </TLSService>
      </TLSSelector>
    </Value>
  </Binding>

  <Binding name="P2_clients" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="192.168.3.2-192.168.3.63" />
        <Port value="any" />
        <Protocol value="tcp" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P2_clients" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="192.168.3.2-192.168.3.63" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
        <TLSVersion value="2.0" />
        <TLSRole value="client" />
      </TLSSelector>
    </Value>
  </Binding>

  <Binding name="P2_ca" type="asset_context_params"
  context="IPsec">
    <Value>
      <IPsecSelector>
        <IPAddress value="192.168.1.122" />
      </IPsecSelector>
    </Value>
  </Binding>

  <Binding name="P2_ca" type="asset_context_params"
  context="TLS">
    <Value>
      <TLSSelector>
        <TLSEndpoint type="local">
          <IPAddress value="192.168.1.122" />
        </TLSEndpoint>
        <TLSVersion value="3.0" />
        <TLSVersion value="2.0" />
      </TLSSelector>
    </Value>
  </Binding>
</GlobalDict>

<PolicyAgreement pla_version="2" this_partner="partner_2">
  <PolicySet interp="conjunct">
    <PolicyRule>
      <Condition>
        <What>
          <Name name="P1_clients" />
        </What>
        <What>
          <Name name="P2_servers" />
        </What>
        <When>
          <Name name="MissionPeriod-1" />
        </When>
      </Condition>

      <Action>
        <ActionElement>
          <Authentication type="data_origin">
            <Name name="auth_level_all-2" />
          </Authentication>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>

        <ActionElement>
          <DataConfidentiality>
            <Name name="cipher_level_all-3" />
          </DataConfidentiality>
          <What role="ca">
            <Name name="P1_ca" />
          </What>
          <What role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>
      </Action>
    </PolicyRule>

    <PolicyRule>
      <Condition>
        <What>
          <Name name="P2_clients" />
        </What>
        <What>
```

```
        <Name name="P1_servers" />
      </What>
      <When>
        <Name name="MissionPeriod-1" />
      </When>
    </Condition>

    <Action>
      <ActionElement>
        <Authentication type="data_origin">
          <Name name="auth_level_all-2" />
        </Authentication>
        <What role="ca">
          <Name name="P1_ca" />
        </What>
        <What role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>

      <ActionElement>
        <DataConfidentiality>
          <Name name="cipher_level_all-3" />
        </DataConfidentiality>
        <What role="ca">
          <Name name="P1_ca" />
        </What>
        <What role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
    </Action>
  </PolicyRule>
</PolicySet>

<Binding name="MissionPeriod-1" type="time">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/20041231T000000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding name="auth_level_all-2"
type="service_mechanism_mapping">
  <Value>
    <AuthenticationExchange>
      <Name name="auth_mech-4" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding name="cipher_level_all-3"
type="service_mechanism_mapping">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="cipher_mech-5" />
    </Encipherment>
  </Value>
</Binding>

<Binding name="auth_mech-4" type="mechanism_context_params"
context="IPsec">
  <Value>
    <EspProposal>
      <IpsecCipher value="AnyAndNull" />
      <IpsecIntegrity value="Any" />
      <IpsecExpiry type="seconds" value="0-3600" />
      <IpsecType value="tunnel" />
    </EspProposal>

    <AhProposal>
      <IpsecIntegrity value="Any" />
      <IpsecExpiry type="seconds" value="0-3600" />
      <IpsecType value="tunnel" />
    </AhProposal>
  </Value>
</Binding>

<Binding name="auth_mech-4" type="mechanism_context_params"
context="TLS">
  <Value>
    <TLSMacAlg value="md5" />
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding name="cipher_mech-5" type="mechanism_context_params"
context="IPsec">
  <Value>
    <EspProposal>
      <IpsecCipher value="Any" />
      <IpsecExpiry type="seconds" value="0-3600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding name="cipher_mech-5" type="mechanism_context_params"
context="TLS">
  <Value>
```

```
        <TLSCipherAlg cipher="rc4" keylength="128" block="false" />
        <TLSCipherAlg cipher="rc4" keylength="40" block="false" />
        <TLSCipherAlg cipher="rc2" keylength="128" block="true" />
        <TLSCipherAlg cipher="rc2" keylength="40" block="true" />
        <TLSCipherAlg cipher="idea" keylength="128" block="true" />
        <TLSCipherAlg cipher="des" keylength="56" block="true" />
        <TLSCipherAlg cipher="des3" keylength="112" block="true" />
      </Value>
    </Binding>
  </PolicyAgreement>
</PLA>
```

D.3 RPLA

PLAs 1 and 2 are resolved to form the following valid RPLA:

```
<?xml version="1.0"?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_1" />
      <Partner name="partner_2" />
    </Coalition>

    <Owner name="partner_1" />

    <Scope partners="partner_1 partner_2" />
  </Head>

  <ResolvedPolicyAgreement rpla_version="0"
  resolver_identity="partner_1">
    <ComponentPLA partner="partner_1" version="1" />
    <ComponentPLA partner="partner_2" version="2" />

    <PolicySet interp="disjunct">
      <PolicySet interp="conjunct">
        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="P1_clients" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="P2_servers" />
            </What>
            <When>
              <Name name="partner_1-bind0" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_1-bind4" />
              </Authentication>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>

            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_1-bind2" />
              </DataConfidentiality>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="P2_clients" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_1-bind5" />
            </What>
            <When>
              <Name name="partner_1-bind0" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_1-bind9" />
              </Authentication>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>

            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_1-bind7" />
              </DataConfidentiality>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
          </Action>
        </PolicyRule>
      </PolicySet>
    </PolicySet>

    <Binding name="P1_servers" type="asset_composition">
      <Value>
        <Name name="P1_servers_80-1" />
        <Name name="P1_servers_443-2" />
      </Value>
    </Binding>

    <Binding name="P1_clients" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.100/16" />
          <Port value="any" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P1_clients" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.100/16" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
          <TLSRole value="client" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="P1_ca" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.0.10.32" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P1_ca" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.0.10.32" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="P2_servers" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="192.168.4.64" />
          <IPAddress value="192.168.2.15" />
          <Port value="443" />
          <Port value="80" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>
```

```
<Binding name="P2_servers" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.4.64" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.2.15" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="443" />
        <Port value="80" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P2_clients" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.3.2-192.168.3.63" />
      <Port value="any" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_clients" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.3.2-192.168.3.63" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
      <TLSRole value="client" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.1.122" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.1.122" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding type="time" name="partner_1-bind0">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/20041231T000000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind4">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind3" />
      <Name name="partner_1-bind3" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind2">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind1" />
      <Name name="partner_1-bind1" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_1-bind5">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="asset_composition" context="TLS"
name="partner_1-bind5">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind9">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind8" />
      <Name name="partner_1-bind8" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind7">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind6" />
      <Name name="partner_1-bind6" />
    </Encipherment>
  </Value>
</Binding>

<Binding name="P1_servers_80-1" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="80" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_servers_80-1" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="80" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="443" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="443" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_1-bind3">
```

```
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="Any" not="false" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind3">
      <Value>
        <TLSMacAlg value="md5" />
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind1">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Any" not="false" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind1">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc4" block="false" keylength="40">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="40">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des" block="true" keylength="56">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind8">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacMd5" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind8">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind6">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind6">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>
  </ResolvedPolicyAgreement>
</PLA>
```

D.4 Reconcile with Correct RPLA

When PLA 1 is reconciled with the correct RPLA shown above, we get the result:

```
bash-2.03$ rplacover.sh pla1.pla rpla
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
.
RPLA RULE //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[2]
RPLA RULE //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[1]
.
-
sets 2 conds 4 acts 2 exprs 10 alts 173895 confs 6 terms 176056 tests 175218
```

The ouput specifies the policy rules in the PLA and RPLA and provides a summary of the work required to check the consistency.

Similarly we get the following when reconciling PLA2 with the RPLA:

```
bash-2.03$ rplacover.sh pla2.pla rpla
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
.
RPLA RULE //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[2]
RPLA RULE //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[1]
.
```

```
-
sets 2 conds 4 acts 2 exprs 10 alts 533358 confs 5 terms 538236 tests 532184
```

D.5 Incorrect RPLA 1

Now, to demonstrate the results of reconcilliation on an invalid RPLA, we modify the RPLA by removing a policy rule as follows:

```
<?xml version="1.0"?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_1" />
      <Partner name="partner_2" />
    </Coalition>

    <Owner name="partner_1" />

    <Scope partners="partner_1 partner_2" />
  </Head>

  <ResolvedPolicyAgreement rpla_version="0"
  resolver_identity="partner_1">
    <ComponentPLA partner="partner_1" version="1" />
    <ComponentPLA partner="partner_2" version="2" />

    <PolicySet interp="disjunct">
      <PolicySet interp="conjunct">
        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="P1_clients" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="P2_servers" />
            </What>
            <When>
              <Name name="partner_1-bind0" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_1-bind4" />
              </Authentication>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>

            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_1-bind2" />
              </DataConfidentiality>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
          </Action>
        </PolicyRule>
      </PolicySet>
    </PolicySet>

    <Binding name="P1_servers" type="asset_composition">
      <Value>
        <Name name="P1_servers_80-1" />
        <Name name="P1_servers_443-2" />
      </Value>
    </Binding>

    <Binding name="P1_clients" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.100/16" />
          <Port value="any" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P1_clients" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.100/16" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
          <TLSRole value="client" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="P1_ca" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="10.0.10.32" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P1_ca" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="10.0.10.32" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="P2_servers" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="192.168.4.64" />
          <IPAddress value="192.168.2.15" />
          <Port value="443" />
          <Port value="80" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P2_servers" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="192.168.4.64" />
          </TLSEndpoint>
          <TLSEndpoint type="local">
            <IPAddress value="192.168.2.15" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
          <TLSVersion value="2.0" />
          <TLSRole value="server" />
          <TLSService>
            <Port value="443" />
            <Port value="80" />
          </TLSService>
        </TLSSelector>
      </Value>
    </Binding>

    <Binding name="P2_clients" type="asset_context_params"
    context="IPsec">
      <Value>
        <IPsecSelector>
          <IPAddress value="192.168.3.2-192.168.3.63" />
          <Port value="any" />
          <Protocol value="tcp" />
        </IPsecSelector>
      </Value>
    </Binding>

    <Binding name="P2_clients" type="asset_context_params"
    context="TLS">
      <Value>
        <TLSSelector>
          <TLSEndpoint type="local">
            <IPAddress value="192.168.3.2-192.168.3.63" />
          </TLSEndpoint>
          <TLSVersion value="3.0" />
          <TLSVersion value="2.0" />
      <TLSRole value="client" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.1.122" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.1.122" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding type="time" name="partner_1-bind0">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/20041231T000000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind4">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind3" />
      <Name name="partner_1-bind3" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind2">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind1" />
      <Name name="partner_1-bind1" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_1-bind5">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="asset_composition" context="TLS"
name="partner_1-bind5">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind9">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind8" />
      <Name name="partner_1-bind8" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind7">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind6" />
      <Name name="partner_1-bind6" />
    </Encipherment>
  </Value>
</Binding>

<Binding name="P1_servers_80-1" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="80" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>
```

```
<Binding name="P1_servers_80-1" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="80" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="443" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="443" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_1-bind3">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="Any" not="false" />
      <IpsecExpiry type="seconds" value="0-3600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_1-bind3">
  <Value>
    <TLSMacAlg value="md5" />
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_1-bind1">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="Any" not="false" />
      <IpsecExpiry type="seconds" value="0-3600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_1-bind1">
  <Value>
    <TLSCipherAlg cipher="rc4" block="false" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc4" block="false" keylength="40">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="128">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="rc2" block="true" keylength="40">
    </TLSCipherAlg>
    <TLSCipherAlg cipher="idea" block="true" keylength="128">
```

```
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des" block="true" keylength="56">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind8">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacMd5" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind8">
      <Value>
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind6">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind6">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>
  </ResolvedPolicyAgreement>
</PLA>
```

D.6 Reconcile with Incorrect RPLA 1

When we reconcile PLA 1 with the modified RPLA 1, then errors are reported:

```
bash-2.03$ rplacover.sh pla1.pla rpla.bad
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
PLA RULE //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
.
RPLA RULE //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[1]
.
-
rule condition not covered
sets 2 conds 2 acts 1 exprs 5 alts 156500 confs 3 terms 156944 tests 155814
```

The output indicates that rule conditions in the PLA are not covered by any rule in the RPLA. This may be the result of a bad PLA or a rule that was excluded by another partner. It is not possible to determine which by looking at the RPLA.

```
bash-2.03$ rplacover.sh pla1.pla rpla.bad
```

Reconciling PLA 2 with the bad RPLA gives similar results.

D.7 Incorrect RPLA 2

In another test, we modified the correct RPLA by changing the supported cipher algorithms:

```
<Binding type="mechanism_context_params" context="IPsec" name="partner_1-bind6">
    <Value>
      <EspProposal choice="Required">
        <IpsecCipher value="Blowfish" not="false"/>
        <IpsecCipher value="Des3" not="false"/>
        <IpsecCipher value="Idea3" not="false"/>
        <IpsecCipher value="Rc5" not="false"/>
        <IpsecCipher value="Rfc1829-iv64" not="false"/>
        <IpsecExpiry type="seconds" value="0-600"/>
        <IpsecType value="tunnel"/>
      </EspProposal>
    </Value>
</Binding>
<Binding type="mechanism_context_params" context="TLS" name="partner_1-bind6">
    <Value>
      <TLSCipherAlg cipher="rc4" block="false" keylength="128">
      </TLSCipherAlg>
      <TLSCipherAlg cipher="rc2" block="true" keylength="128">
      </TLSCipherAlg>
      <TLSCipherAlg cipher="idea" block="true" keylength="128">
      </TLSCipherAlg>
      <TLSCipherAlg cipher="des3" block="true" keylength="112">
      </TLSCipherAlg>
    </Value>
</Binding>
```

Becomes:

```
<Binding type="mechanism_context_params" context="IPsec" name="partner_1-bind6">
    <Value>
      <EspProposal choice="Required">
        <IpsecCipher value="Des" not="false"/>
        <IpsecCipher value="Idea" not="false"/>
        <IpsecExpiry type="seconds" value="0-600"/>
        <IpsecType value="tunnel"/>
      </EspProposal>
    </Value>
</Binding>
<Binding type="mechanism_context_params" context="TLS" name="partner_1-bind6">
    <Value>
      <TLSCipherAlg cipher="des" block="true" keylength="56">
      </TLSCipherAlg>
    </Value>
</Binding>
```

D.8 Reconcile with Incorrect RPLA 2

The second incorrect RPLA conflicts with the policies in PLA 1. Reconciling it gives the following results:

```
bash-2.03$ rplacover.sh pla1.pla rpla2.bad
PLA     RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
PLA     RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
.
RPLA    RULE    //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[2]
RPLA    RULE    //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[1]
.
-
condition       IS rhs.IPAddress(10.0.10.2)     //PLA[1]/ResolvedPolicyAgreement[1]/Binding[19]/Value[1]/IPsecSelector[1]/IPAddress[3]
condition       IS rhs.Port(80) //PLA[1]/ResolvedPolicyAgreement[1]/Binding[19]/Value[1]/IPsecSelector[1]/Port[1]
condition       IS rhs.Protocol(tcp)    //PLA[1]/ResolvedPolicyAgreement[1]/Binding[19]/Value[1]/IPsecSelector[1]/Protocol[1]
condition       LE lhs.IPAddress(192.168.3.63)  //PLA[1]/ResolvedPolicyAgreement[1]/Binding[8]/Value[1]/IPsecSelector[1]/IPAddress[1]
condition       GE lhs.IPAddress(192.168.3.2)   //PLA[1]/ResolvedPolicyAgreement[1]/Binding[8]/Value[1]/IPsecSelector[1]/IPAddress[1]
condition       IS lhs.Protocol(tcp)    //PLA[1]/ResolvedPolicyAgreement[1]/Binding[8]/Value[1]/IPsecSelector[1]/Protocol[1]
condition       LE TimeRange(1104451200)        //PLA[1]/ResolvedPolicyAgreement[1]/Binding[12]/Value[1]/TimePeriod[1]/TimeRange[1]
condition       GE TimeRange(978325200) //PLA[1]/ResolvedPolicyAgreement[1]/Binding[12]/Value[1]/TimePeriod[1]/TimeRange[1]
.
action  ISNT TLSCipherAlg.cipher(des3)  //PLA[1]/PolicyAgreement[1]/Binding[13]/Value[1]/TLSCipherAlg[4]
action  ISNT TLSCipherAlg.cipher(idea)  //PLA[1]/PolicyAgreement[1]/Binding[13]/Value[1]/TLSCipherAlg[3]
action  ISNT TLSCipherAlg.cipher(rc2)   //PLA[1]/PolicyAgreement[1]/Binding[13]/Value[1]/TLSCipherAlg[2]
action  ISNT TLSCipherAlg.cipher(rc4)   //PLA[1]/PolicyAgreement[1]/Binding[13]/Value[1]/TLSCipherAlg[1]
action  ISNT role(ca)   //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]/Action[1]/ActionElement[1]/What[1]
action  ISNT TLSMacAlg(sha)     //PLA[1]/PolicyAgreement[1]/Binding[11]/Value[1]/TLSMacAlg[1]
action  ISNT IpsecIntegrity(HmacMd5)    //PLA[1]/PolicyAgreement[1]/Binding[10]/Value[1]/EspProposal[1]/IpsecIntegrity[1]
action  ISNT IpsecIntegrity(HmacSha1)   //PLA[1]/PolicyAgreement[1]/Binding[10]/Value[1]/EspProposal[1]/IpsecIntegrity[2]
action  IS IpsecCipher(Idea)    //PLA[1]/ResolvedPolicyAgreement[1]/Binding[29]/Value[1]/EspProposal[1]/IpsecCipher[2]
action  IS IpsecExpiry()        //PLA[1]/ResolvedPolicyAgreement[1]/Binding[29]/Value[1]/EspProposal[1]/IpsecExpiry[1]
action  IS IpsecType(tunnel)    //PLA[1]/ResolvedPolicyAgreement[1]/Binding[29]/Value[1]/EspProposal[1]/IpsecType[1]
.
rule actions are not covered
sets 2  conds 3 acts 2  exprs 11 alts 157354 confs 8 terms 158327 tests 157020
```

The output indicates that there was a problem with the actions and indicates which rule caused the conflict.

The changes to the RPLA do not conflict with PLA 2, however. They just limit the acceptable policy in a different manner that the correct RPLA.

```
bash-2.03$ rplacover.sh pla2.pla rpla2.bad
PLA     RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[2]
PLA     RULE    //PLA[1]/PolicyAgreement[1]/PolicySet[1]/PolicyRule[1]
.
RPLA    RULE    //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[2]
RPLA    RULE    //PLA[1]/ResolvedPolicyAgreement[1]/PolicySet[1]/PolicySet[1]/PolicyRule[1]
.
-
sets 2 conds 4 acts 2 exprs 10 alts 414978 confs 5 terms 419724 tests 414236
```

E PLAL to SPSL Conversion

This appendix shows an example of the PLAL to SPSL converter converting an RPLA to an SPSL that can be imported into a PBSM system to use for policy negotiation. Note that SPSL does not support TLS policies, so they are dropped in the conversion. Also items like signatures are currently not supported in the prototype. The RPLA used results from resolving the policies in the example provided in the MSME release in plal-examples/demo/system.

E.1 RPLA in PLAL

```
<?xml version="1.0"?>
<!DOCTYPE PLA PUBLIC "-//BBN/DTD MSME PLAL v0.2//EN" "plal1.dtd">
<PLA>
  <Head>
    <Coalition name="secret_mission">
      <Partner name="partner_1" />
      <Partner name="partner_2" />
      <Partner name="partner_3" />
    </Coalition>

    <Owner name="partner_1" />

    <Scope partners="partner_1 partner_2 partner_3" />
  </Head>

  <ResolvedPolicyAgreement rpla_version="0"
  resolver_identity="partner_1">
    <ComponentPLA partner="partner_1" version="1" />
    <ComponentPLA partner="partner_3" version="1" />
    <ComponentPLA partner="partner_2" version="2" />

    <PolicySet interp="disjunct">
      <PolicySet interp="conjunct">
        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="P2_clients" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="partner_1-bind43" />
            </What>
            <When>
              <Name name="partner_1-bind23" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_1-bind49" />
              </Authentication>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_1-bind46" />
              </DataConfidentiality>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
          </Action>
        </PolicyRule>

        <PolicyRule>
          <Condition>
            <What direction="both" type="any" role="none">
              <Name name="P1_clients" />
            </What>
            <What direction="both" type="any" role="none">
              <Name name="P2_servers" />
            </What>
            <When>
              <Name name="partner_1-bind23" />
            </When>
          </Condition>

          <Action>
            <ActionElement>
              <Authentication type="data_origin" choice="Required">
                <Name name="partner_1-bind55" />
              </Authentication>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
            <ActionElement>
              <DataConfidentiality type="connectionless"
              choice="Required">
                <Name name="partner_1-bind52" />
              </DataConfidentiality>
              <What direction="both" type="any" role="ca">
                <Name name="P1_ca" />
              </What>
              <What direction="both" type="any" role="ca">
                <Name name="P2_ca" />
              </What>
            </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="P1_agents" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="P2_agents" />
    </What>
    <When>
      <Name name="partner_1-bind23" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind59" />
      </Authentication>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_1-bind60" />
      </DataConfidentiality>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="P3_agents" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_1-bind10" />
    </What>
    <When>
      <Name name="MissionPeriod-1" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind68" />
      </Authentication>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_1-bind66" />
      </DataConfidentiality>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="partner_1-bind14" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="P3_agents" />
    </What>
    <When>
      <Name name="MissionTime-3" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind18" />
      </Authentication>
```

```
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
      <ActionElement>
        <DataConfidentiality type="connectionless"
        choice="Required">
          <Name name="partner_1-bind16" />
        </DataConfidentiality>
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
    </Action>
  </PolicyRule>
</PolicySet>

<PolicySet interp="conjunct">
  <PolicyRule>
    <Condition>
      <What direction="both" type="any" role="none">
        <Name name="P2_clients" />
      </What>
      <What direction="both" type="any" role="none">
        <Name name="partner_1-bind78" />
      </What>
      <When>
        <Name name="partner_1-bind23" />
      </When>
    </Condition>

    <Action>
      <ActionElement>
        <Authentication type="data_origin" choice="Required">
          <Name name="partner_1-bind80" />
        </Authentication>
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
      <ActionElement>
        <DataConfidentiality type="connectionless"
        choice="Required">
          <Name name="partner_1-bind79" />
        </DataConfidentiality>
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
    </Action>
  </PolicyRule>

  <PolicyRule>
    <Condition>
      <What direction="both" type="any" role="none">
        <Name name="P1_clients" />
      </What>
      <What direction="both" type="any" role="none">
        <Name name="P2_servers" />
      </What>
      <When>
        <Name name="partner_1-bind23" />
      </When>
    </Condition>

    <Action>
      <ActionElement>
        <Authentication type="data_origin" choice="Required">
          <Name name="partner_1-bind82" />
        </Authentication>
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
      <ActionElement>
        <DataConfidentiality type="connectionless"
        choice="Required">
          <Name name="partner_1-bind81" />
        </DataConfidentiality>
        <What direction="both" type="any" role="ca">
          <Name name="P1_ca" />
        </What>
        <What direction="both" type="any" role="ca">
          <Name name="P2_ca" />
        </What>
      </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="P1_agents" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="P2_agents" />
    </What>
    <When>
      <Name name="partner_1-bind23" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind89" />
      </Authentication>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_1-bind91" />
      </DataConfidentiality>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="P3_agents" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="partner_1-bind10" />
    </What>
    <When>
      <Name name="MissionPeriod-1" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind68" />
      </Authentication>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
    <ActionElement>
      <DataConfidentiality type="connectionless"
      choice="Required">
        <Name name="partner_1-bind66" />
      </DataConfidentiality>
      <What direction="both" type="any" role="ca">
        <Name name="P1_ca" />
      </What>
      <What direction="both" type="any" role="ca">
        <Name name="P2_ca" />
      </What>
    </ActionElement>
  </Action>
</PolicyRule>

<PolicyRule>
  <Condition>
    <What direction="both" type="any" role="none">
      <Name name="partner_1-bind22" />
    </What>
    <What direction="both" type="any" role="none">
      <Name name="P3_agents" />
    </What>
    <When>
      <Name name="MissionTime-3" />
    </When>
  </Condition>

  <Action>
    <ActionElement>
      <Authentication type="data_origin" choice="Required">
        <Name name="partner_1-bind18" />
      </Authentication>
          <What direction="both" type="any" role="ca">
            <Name name="P1_ca" />
          </What>
          <What direction="both" type="any" role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>
        <ActionElement>
          <DataConfidentiality type="connectionless"
          choice="Required">
            <Name name="partner_1-bind16" />
          </DataConfidentiality>
          <What direction="both" type="any" role="ca">
            <Name name="P1_ca" />
          </What>
          <What direction="both" type="any" role="ca">
            <Name name="P2_ca" />
          </What>
        </ActionElement>
      </Action>
    </PolicyRule>
  </PolicySet>
</PolicySet>

<Binding name="P1_servers" type="asset_composition">
  <Value>
    <Name name="P1_servers_80-1" />
    <Name name="P1_servers_443-2" />
  </Value>
</Binding>

<Binding name="P1_clients" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.100/16" />
      <Port value="any" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_clients" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.100/16" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="client" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P1_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.100/16" />
      <Port value="22" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_agents" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.100/16" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="client" />
      <TLSService>
        <Port value="22" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P1_ca" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.10.32" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_ca" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.32" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
    </TLSSelector>
  </Value>
```

```
</Binding>

<Binding name="P2_servers" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.4.64" />
      <IPAddress value="192.168.2.15" />
      <Port value="443" />
      <Port value="80" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_servers" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.4.64" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.2.15" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="443" />
        <Port value="80" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P2_clients" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.3.2-192.168.3.63" />
      <Port value="any" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_clients" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.3.2-192.168.3.63" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
      <TLSRole value="client" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P2_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.3.2-192.168.3.63" />
      <Port value="20-22" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.168.1.122" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P2_ca" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="192.168.1.122" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSVersion value="2.0" />
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P3_agents" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="192.169.0.0-192.169.10.255" />
      <Port value="20-22" />
      <Protocol value="tcp" />
```

```
    </IPsecSelector>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_1-bind43">
  <Value>
    <Name name="partner_1-bind42" />
    <Name name="partner_1-bind41" />
  </Value>
</Binding>

<Binding type="time" name="partner_1-bind23">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/20041231T000000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind49">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind48" />
      <Name name="partner_1-bind47" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind46">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind45" />
      <Name name="partner_1-bind44" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind55">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind54" />
      <Name name="partner_1-bind53" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind52">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind51" />
      <Name name="partner_1-bind50" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind59">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind53" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind60">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind50" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_1-bind10">
  <Value>
    <Name name="P2_agents" />
  </Value>
</Binding>

<Binding name="MissionPeriod-1" type="time">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/20041231T000000" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind68">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind67" />
    </AuthenticationExchange>
  </Value>
</Binding>
```

```
<Binding type="service_mechanism_mapping"
name="partner_1-bind66">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind65" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_1-bind14">
  <Value>
    <Name name="partner_1-bind11" />
    <Name name="partner_1-bind12" />
  </Value>
</Binding>

<Binding name="MissionTime-3" type="time">
  <Value>
    <TimePeriod>
      <TimeRange value="20010101T050000/THISANDFUTURE" />
    </TimePeriod>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind18">
  <Value>
    <AuthenticationExchange>
      <Name name="partner_1-bind17" />
    </AuthenticationExchange>
  </Value>
</Binding>

<Binding type="service_mechanism_mapping"
name="partner_1-bind16">
  <Value>
    <Encipherment type="reversible_symmetric">
      <Name name="partner_1-bind15" />
    </Encipherment>
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_1-bind78">
  <Value>
    <Name name="partner_1-bind77" />
    <Name name="partner_1-bind76" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind80">
  <Value>
    <Name name="partner_1-bind55" />
    <Name name="partner_1-bind59" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind79">
  <Value>
    <Name name="partner_1-bind52" />
    <Name name="partner_1-bind60" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind82">
  <Value>
    <Name name="partner_1-bind55" />
    <Name name="partner_1-bind59" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind81">
  <Value>
    <Name name="partner_1-bind52" />
    <Name name="partner_1-bind60" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind89">
  <Value>
    <Name name="partner_1-bind88" />
    <Name name="partner_1-bind59" />
  </Value>
</Binding>

<Binding type="service_composition" name="partner_1-bind91">
  <Value>
    <Name name="partner_1-bind90" />
    <Name name="partner_1-bind60" />
  </Value>
</Binding>

<Binding type="asset_composition" name="partner_1-bind22">
  <Value>
    <Name name="partner_1-bind11" />
    <Name name="partner_1-bind12" />
  </Value>
</Binding>

<Binding name="P1_servers_80-1" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="80" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_servers_80-1" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="80" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="IPsec">
  <Value>
    <IPsecSelector>
      <IPAddress value="10.0.1.24" />
      <IPAddress value="10.0.3.164" />
      <IPAddress value="10.0.10.2" />
      <Port value="443" />
      <Protocol value="tcp" />
    </IPsecSelector>
  </Value>
</Binding>

<Binding name="P1_servers_443-2" type="asset_context_params"
context="TLS">
  <Value>
    <TLSSelector>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.1.24" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.3.164" />
      </TLSEndpoint>
      <TLSEndpoint type="local">
        <IPAddress value="10.0.10.2" />
      </TLSEndpoint>
      <TLSVersion value="3.0" />
      <TLSRole value="server" />
      <TLSService>
        <Port value="443" />
      </TLSService>
    </TLSSelector>
  </Value>
</Binding>

<Binding type="asset_composition" context="TLS"
name="partner_1-bind42">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="asset_composition" context="IPsec"
name="partner_1-bind41">
  <Value>
    <Name name="P1_servers_80-1" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="TLS"
name="partner_1-bind48">
  <Value>
    <TLSMacAlg value="sha" />
  </Value>
</Binding>

<Binding type="mechanism_context_params" context="IPsec"
name="partner_1-bind47">
  <Value>
    <EspProposal choice="Required">
      <IpsecCipher value="AnyAndNull" not="false" />
      <IpsecIntegrity value="HmacMd5" not="false" />
      <IpsecIntegrity value="HmacSha1" not="false" />
      <IpsecExpiry type="seconds" value="0-600" />
      <IpsecType value="tunnel" />
    </EspProposal>
  </Value>
</Binding>
```

```
    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind45">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind44">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Blowfish" not="false" />
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecCipher value="Rc5" not="false" />
          <IpsecCipher value="Rfc1829-iv64" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind54">
      <Value>
        <TLSMacAlg value="md5" />
        <TLSMacAlg value="sha" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind53">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="Any" not="false" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="TLS"
    name="partner_1-bind51">
      <Value>
        <TLSCipherAlg cipher="rc4" block="false" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc4" block="false" keylength="40">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="rc2" block="true" keylength="40">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="idea" block="true" keylength="128">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des" block="true" keylength="56">
        </TLSCipherAlg>
        <TLSCipherAlg cipher="des3" block="true" keylength="112">
        </TLSCipherAlg>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind50">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Any" not="false" />
          <IpsecExpiry type="seconds" value="0-3600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind67">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind65">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="asset_composition" context="IPsec"
    name="partner_1-bind11">
      <Value>
        <Name name="P1_agents" />
      </Value>
    </Binding>

    <Binding type="asset_composition" context="TLS"
    name="partner_1-bind12">
      <Value>
        <Name name="P1_agents" />
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind17">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="AnyAndNull" not="false" />
          <IpsecIntegrity value="HmacSha1" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="mechanism_context_params" context="IPsec"
    name="partner_1-bind15">
      <Value>
        <EspProposal choice="Required">
          <IpsecCipher value="Des3" not="false" />
          <IpsecCipher value="Idea3" not="false" />
          <IpsecExpiry type="seconds" value="0-600" />
          <IpsecType value="tunnel" />
        </EspProposal>
      </Value>
    </Binding>

    <Binding type="asset_composition" context="TLS"
    name="partner_1-bind77">
      <Value>
        <Name name="P1_servers_443-2" />
      </Value>
    </Binding>

    <Binding type="asset_composition" context="IPsec"
    name="partner_1-bind76">
      <Value>
        <Name name="P1_servers_443-2" />
      </Value>
    </Binding>

    <Binding type="service_mechanism_mapping"
    name="partner_1-bind88">
      <Value>
        <AuthenticationExchange>
          <Name name="partner_1-bind53" />
        </AuthenticationExchange>
      </Value>
    </Binding>

    <Binding type="service_mechanism_mapping"
    name="partner_1-bind90">
      <Value>
        <Encipherment type="reversible_symmetric">
          <Name name="partner_1-bind50" />
        </Encipherment>
      </Value>
    </Binding>
  </ResolvedPolicyAgreement>
</PLA>
```

E.2 RPLA Converted to SPSL

```
# SPSL Converted via plal2spsl
# _Id: plal2spsl.c,v 1.8 2001/11/08 16:39:15 djw Exp _#
policy-name: policyName0
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 192.168.3.2-192.168.3.63 \
port any \
src 10.0.1.24,10.0.3.164,10.0.10.2 \
port 80 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher blowfish,des3,idea3,rc5,rfc1829-iv64 \
integrity any  \
expiry seconds 0-600 \
tunnel \
ah req integrity hmacmd5 expiry seconds 0-600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 486aaaa38961

policy-name: policyName1
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port any \
src 192.168.4.64,192.168.2.15 \
port 443,80 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher any \
integrity any  \
expiry seconds 0-3600 \
tunnel \
ah req integrity any expiry seconds 0-3600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 439aaaa35459

policy-name: policyName2
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port 22 \
src 192.168.3.2-192.168.3.63 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher any \
integrity any  \
expiry seconds 0-3600 \
tunnel \
ah req integrity any expiry seconds 0-3600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 436aaaa35120

policy-name: policyName3
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 192.169.0.0-192.169.10.255 \
port 20-22 \
src 192.168.3.2-192.168.3.63 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher des3,idea3 \
integrity any  \
expiry seconds 0-600 \
tunnel \
ah req integrity hmacsha1 expiry seconds 0-600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 462aaaa36821

policy-name: policyName4
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port 22 \
src 192.169.0.0-192.169.10.255 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher des3,idea3 \
integrity any  \
expiry seconds 0-600 \
tunnel \
ah req integrity hmacsha1 expiry seconds 0-600 \
tunnel \
```

```
mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 448aaaa36097

policy-name: policyName5
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 192.168.3.2-192.168.3.63 \
port any \
src 10.0.1.24,10.0.3.164,10.0.10.2 \
port 443 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher any \
integrity any  \
expiry seconds 0-3600 \
tunnel \
ah req integrity any expiry seconds 0-3600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 452aaaa36078

policy-name: policyName6
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port any \
src 192.168.4.64,192.168.2.15 \
port 443,80 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher any \
integrity any  \
expiry seconds 0-3600 \
tunnel \
ah req integrity any expiry seconds 0-3600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 439aaaa35464

policy-name: policyName7
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port 22 \
src 192.168.3.2-192.168.3.63 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher any \
integrity any  \
expiry seconds 0-3600 \
tunnel \
ah req integrity any expiry seconds 0-3600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 436aaaa35125

policy-name: policyName8
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 192.169.0.0-192.169.10.255 \
port 20-22 \
src 192.168.3.2-192.168.3.63 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher des3,idea3 \
integrity any  \
expiry seconds 0-600 \
tunnel \
ah req integrity hmacsha1 expiry seconds 0-600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 462aaaa36826

policy-name: policyName9
notes: PLA version 0
# association: Unknown
cache-expiry: 0
policy: \
dst 10.100.0.0/16 \
port 22 \
src 192.169.0.0-192.169.10.255 \
port 20-22 \
xport-proto 6 \
direction inbound, symmetric permit
ipsec-action: \
esp req  cipher des3,idea3 \
integrity any  \
expiry seconds 0-600 \
tunnel \
ah req integrity hmacsha1 expiry seconds 0-600 \
tunnel \

mnt-by: plal2spsl
changed: plal2spsl.for.partner_1 20020227
signature: MAKEUP MAKEUP-CERT rsa-pkcs1 448aaaa3610
```